PROJECTE FINAL DE CARRERA

Sistema de Gestión de Continuidad de Negocio de Call Center

(Call Center Business Continuity Management System)

Estudis: Enginyeria de Telecomunicació

Autor: Angel Ortega Moreno

Director/a: Jaume Mussons Selles

Any: 2016

Índice general

Índice general 1
Colaboraciones 3
Resum del Projecte 4
Resumen del Proyecto 6
Abstract 8
1. Introducción 10
1.1 Contexto del proyecto 10
1.2 Objetivos 11
1.3 Estructura de la memoria 11
2. Metodologia 13
2.1 Descripción del proceso de implantación 13
2.1.1. Contexto 14
2.1.2. Liderazgo 15
2.1.3. Planificación 16
2.1.4. Soporte 18
2.1.5. Operación 19
2.1.6. Evaluación 24
2.1.7. Mejora 26
3. Caso Práctico 28
3.1 Contexto del proyecto 28
3.2 Alcance 28
3.3 Planificación 30
3.4 Compromiso del Promotor 33
3.5 Análisis de Contexto 34
3.6 Análisis de Impacto de Negocio 37
3.7 Liderazgo 40
3.7.1. Estado de normalidad 41
3.7.2. Gestión de incidentes 47

3.7.3. Gestión de crisis 51
3.8 Política de Continuidad y Objetivos Estratégicos 57
3.9 Análisis de Riesgos 58
3.10 Concienciación y formación 64
3.11 Estrategias de continuidad 66
3.12 Planes y procedimientos de continuidad de negocio 68
3.13 Pruebas 69
3.14 Evaluación del SGCN 72
3.15 Mejora 73
4. Conclusiones 75
5. Anexos 76
5.1 Amenazas y vulnerabilidades 76
5.2 Estrategias de recuperación del CPD 76
5.3 Estrategias de recuperación de datos 78
6. Referencias 80

Colaboraciones

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Departament d'Organització d'Empreses

Price Waterhouse Coopers

Resum del Projecte

La continuïtat de negoci s'emmarca dins la gestió de riscos d'indisponiblitat dels processos de negoci crítics per una organització. Dóna cobertura a la totalitat d'actius que donen suport als esmentats processos de negoci, és a dir, tots aquells actius sense els quals seria impossible dur a terme les tasques i fases per les quals transcorren els processos de negoci dins de l'abast delimitat.

Dins de la gestió de la continuïtat de negoci s'inclouen molts altres plans o processos de seguretat i continuïtat en els quals les organitzacions porten temps destinant recursos, generalment. Alguns exemples d'aquests plans o processos són: manuals d'autoprotecció d'edificis o seus, plans d'emergències i evacuació, plans de contingències informàtiques, plans de recuperació de desastres, etc.

El propòsit de la continuïtat de negoci és identificar i protegir els processos de negoci crítics i els recursos requerits pels mateixos per mantenir un nivell acceptable de les seves operacions, salvaguardant aquests recursos i preparant procediments per assegurar la supervivència de les operacions crítiques de l'organització en cas d'incidència, contingència o desastre.

Un Sistema de Gestió de Continuïtat de Negoci (d'ara endavant, SGCN) té en compte tot aquest plantejament, tenint-ho com a base, encara que afegeix una sèrie d'accions i exercicis que han de repetir-se de manera periòdica o enfront de canvis significatius en l'organització, de manera que s'asseguri l'alineament de la realitat de l'organització vers tota la documentació, plans, procediments i protocols dissenyats en la fase de disseny i presa de requeriments del projecte. Així mateix, el SGCN s'ha desenvolupat tenint com a referència la norma ISO 22301, que estableix un cicle de millora contínua en els cicles periòdics o sorgits a causa de canvis significatius en l'organització.

La importància en la continuïtat de negoci fa focus en la incertesa que les organitzacions tenen front l'ocurrència d'una contingència o desastre. Encara que la magnitud i el moment d'ocurrència d'una contingència o desastre no es poden predir, es pot afirmar que totes les organitzacions

estan exposades a ells i cal esperar que tard o d'hora, aquests tinguin afectació sobre l'operació dels processos de negoci que desenvolupa l'organització.

Si es té en compte la continuïtat de negoci i la seva gestió, s'aconsegueix que l'afectació sobre l'organització sigui acceptable, en funció dels recursos que es puguin destinar a aplicar la salvaguardes necessàries per minimitzar aquesta afectació. D'aquesta manera es poden aconseguir objectius de reducció d'1) la pèrdua de la imatge de l'organització enfront dels seus clients, usuaris i altres parts interessades, 2) l'impacte legal, per les obligacions regulatòries sectorials o d'aplicabilitat generalitzada a la qual estan subjectes les organitzacions i 3) les pèrdues econòmiques derivades d'una interrupció en els serveis que presten les organitzacions, donat una fallada en els processos de negoci crítics a causa d'una contingència o desastre.

El projecte s'ha abordat en les fases que descriu el cicle de DEMING (Planificació-PLA, Execució-DO, Validació-CHECK i Reacció-ACT) i tenint en compte les directrius que la norma ISO 22301 ofereix sobre l'estructura d'implantació i manteniment d'un SGCN, sent l'exercici final del primer cicle la certificació de la validesa i efectivitat del SGCN per part d'una entitat externa independent i de reconeixement internacional.

Resumen del Proyecto

La continuidad de negocio se enmarca dentro de la gestión de riesgos de indisponibilidad de los procesos de negocio críticos para una organización. Da cobertura a la totalidad de activos que dan soporte a los mencionados procesos de negocio, es decir, todos aquellos activos sin los cuales sería imposible llevar a cabo las tareas y fases por las que transcurren los procesos de negocio dentro del alcance delimitado.

Dentro de la gestión de la continuidad de negocio se incluyen muchos otros planes o procesos de seguridad y continuidad en los que las organizaciones llevan tiempo destinando recursos, generalmente. Algunos ejemplos de estos planes o procesos son: manuales de autoprotección de edificios o sedes, planes de emergencias y evacuación, planes de contingencias informáticas, planes de recuperación de desastres, etc.

El propósito de la continuidad de negocio es identificar y proteger los procesos de negocio críticos y los recursos requeridos por los mismos para mantener un nivel aceptable de sus operaciones, salvaguardando estos recursos y preparando procedimientos para asegurar la supervivencia de las operaciones críticas de la organización en caso de incidencia, contingencia o desastre.

Un Sistema de Gestión de Continuidad de Negocio (en adelante, SGCN) tiene en cuenta todo este planteamiento, teniéndolo como base, aunque añade una serie de acciones y ejercicios que deben repetirse de manera periódica o frente a cambios significativos en la organización, de manera que se asegure la alineación de la realidad de la organización conforme a toda la documentación, planes, procedimientos y protocolos diseñados en la fase de diseño y toma de requisitos del proyecto. Asimismo, el SGCN se ha desarrollado teniendo como referencia la norma ISO 22301, que establece un ciclo de mejora continua en los ciclos periódicos o surgidos a causa de cambios significativos en la organización.

La importancia en la continuidad de negocio recaba en la incertidumbre que las organizaciones tienen frente la ocurrencia de una contingencia o desastre. Aunque la magnitud y el momento de ocurrencia de una contingencia o desastre no se pueden predecir, se puede afirmar que todas las organizaciones están expuestas a ellos y cabe esperar que tarde o temprano, estos tengan afectación sobre la operación de los procesos de negocio que desarrolla la organización.

Si se tiene en cuenta la continuidad de negocio y su gestión, se consigue que la afectación sobre la organización sea aceptable, en función de los recursos que se puedan destinar a aplicar la salvaguardas necesarias para minimizar esta afectación. De esta manera se pueden alcanzar objetivos de reducción de 1) la pérdida de la imagen de la organización frente a sus clientes, usuarios y demás partes interesadas, 2) el impacto legal, por las obligaciones regulatorias sectoriales o de aplicabilidad generalizada a la que están sujetas las organizaciones y 3) las pérdidas económicas derivadas de una interrupción en los servicios que prestan las organizaciones, dado un fallo en los procesos de negocio críticos a causa de una contingencia o desastre.

El proyecto se ha abordado en las fases que describe el ciclo de DEMING (Planificación-PLAN, Ejecución-DO, Validación-CHECK y Reacción-ACT) y teniendo en cuenta las directrices que la norma ISO 22301 ofrece sobre la estructura de implantación y mantenimiento de un SGCN, siendo el ejercicio final del primer ciclo la certificación de la validez y efectividad del SGCN por parte de una entidad externa independiente y de reconocimiento internacional.

Abstract

Business continuity is part of the unavailability risk management of critical business processes for an organization. It provides coverage for all assets that support the above business processes, that means, all those assets without which it would be impossible to carry out the tasks and phases through which pass the business processes within the defined scope.

Within the management of business continuity it is included many other plans or safety and continuity processes in which organizations have long allocating resources generally. Examples of these plans or processes are manual self-protection of buildings or offices, emergency and evacuation plans, computing contingency plans, disaster recovery plans, etc.

The purpose of business continuity is to identify and protect critical business processes and resources required for them to maintain an acceptable level of operations, safeguarding these resources and preparing procedures to ensure the survival of the critical operations of the organization event of an incident, contingency or disaster.

Business Continuity Management System (hereinafter BCMS) takes into account this whole approach, using it as a basis, but adds a series of actions and exercises that should be repeated periodically or when significant changes occur in the organization so the alignment of the reality of the organization according to all the documentation, plans, procedures and protocols designed in the design phase and decision ensure project requirements. Also, the BCMS has been developed in reference to the ISO 22301 standard, which establishes a continuous improvement periodical cycles or arising because of significant changes in the organization cycles.

The importance on business continuity is collected in uncertainty that organizations have against the occurrence of a contingency or disaster. Although the magnitude and time of occurrence of a contingency or disaster cannot be predicted, it could be said that all organizations are exposed to them and it is expected that sooner or later these have

negative effects on the operation of business processes that the organization develops.

Taking into account the continuity of business and management, the impact on the organization is acceptable, depending on the resources that can be allocated to implement the necessary safeguards to minimize this involvement. By this means it can be achieved to reduce 1) loss of image of the organization with its customers, users and other interested parties, 2) the legal impact, sectorial regulatory obligations or generalized applicability to which the organizations are subject and 3) economic losses resulting from a disruption in the services provided by the organizations, given a failure in critical business processes because of a contingency or disaster.

The project has been addressed in phases describing the cycle DEMING (Planning-PLAN, Run-DO, Validation-CHECK and Reaction-ACT) and taking into account the guidelines ISO 22301 provides on the structure of implementation and maintenance a BCMS, being the final exercise of the first yearly certification cycle of the validity and effectiveness of the BCMS by an independent external and international recognized entity.

1. Introducción

Cualquier organización está expuesta a ciertas amenazas que exponen a sus procesos de negocio críticos a su interrupción, siendo su tipología analizable y clasificable en cuanto al impacto de su reputación ante sus clientes y competidores así como las repercusiones económicas, legales o regulatorias.

Un Sistema de Gestión de Continuidad de Negocio tiene en cuenta todas estas variables en base a las directrices marcadas en la norma ISO22301, que permite tener en cuenta todos los activos pertenecientes a la organización, así como todo su contexto y relación con partes interesadas en su negocio.

Mediante la implantación de un sistema como el que se describe a lo largo del proyecto se asegura la resistencia y continuidad de los procesos críticos de negocio, consiguiendo la fácil y efectiva toma de decisiones en situaciones de crisis, a la vez que se mejora la confianza de los clientes y se adquiere un ahorro de costes en la gestión de los activos de la organización.

1.1 Contexto del proyecto

El proyecto permite establecer implantación de SGCN en organizaciones en las que se considere necesario invertir en continuidad de negocio en procesos relacionados con atención de llamadas en un amplio espectro del sector. El alcance planteado da cabida a organizaciones que tengan área de preventa o postventa telefónica, servicio al cliente (servicios de seguridad, asistencia de seguros), o se dediquen exclusivamente a la atención de llamadas dando servicio a otras entidades (estudios de mercado, campañas de marketing) o de manera directa al como servicio público (teléfonos de información o emergencias).

Son analizados todos los agentes internos y externos que puedan afectar a los procesos de negocio, según sus necesidades y requerimientos, teniendo en cuenta activos TIC, todos los proveedores participantes, las instalaciones y las personas que operan los procesos de negocio.

El proyecto presentado en el presente PFC parte del mencionado análisis y analiza sistemáticamente los riesgos de continuidad existentes en función de las necesidades del negocio (tiempo de interrupción

permitido, pérdida de datos permitida, acuerdos de nivel de servicio, regulaciones o leyes, etc.) y permite establecer medidas y estrategias para mitigarlos en ciclos sucesivos de mejora continua de manera priorizada en función de los recursos de los que se disponga.

1.2 Objetivos

Un Sistema de Gestión de Continuidad de Negocio (en adelante SGCN) establece un ciclo de mejora continua que permite que los procedimientos, políticas y procesos se mantengan actualizados a la situación real de la entidad que lo implanta. Se garantiza que los objetivos de continuidad fijados por la entidad se satisfagan y que la respuesta frente a situaciones desfavorables sea eficiente y eficaz.

El SGCN presentado se centra en asegurar la continuidad de los procesos de negocio críticos para entidades que basen su negocio total o parcialmente en la atención de llamadas, es decir, que dispongan de un call center.

Los objetivos principales del proyecto son:

- Proporcionar una ventaja competitiva de la entidad que implanta el SGCN.
- Preservación de la imagen de la marca de la entidad que implanta el SGCN.
- Ahorrar costes gracias al análisis globalizado que se lleva a cabo.
- Asegurar el cumplimiento de las regulaciones aplicables a los procesos dentro del alcance del SGCN.
- Tratamiento de riesgos de reputación, legales y de interrupción de los procesos críticos.

Se describe de manera generalista, aunque indicando las peculiaridades según el negocio y la criticidad del servicio prestado por el call center en el que se deba implantar el SGCN.

1.3 Estructura de la memoria

La memoria del proyecto se ha realizado siguiendo los estándares de la UPC para la presentación de proyectos de final de carrera.

Primeramente, después de la los agradecimientos, el resumen del proyecto y la presente introducción, se presenta de manera extensa la metodología utilizada

durante el proyecto, describiendo y justificando las tareas llevadas a cabo y las herramientas de consolidación de información empleadas en cada una de las fases.

A continuación se dedica un capítulo a la exposición del trabajo a llevar a cabo para aplicar la metodología a los diferentes casos a modo de caso práctico. En dicho capítulo se describen los puntos más significativos y relevantes dentro del proceso de implantación de un SGCN, el trabajo completo puede verse en los diferentes anexos.

El tercer capítulo contiene los resultados que se obtienen a partir de la implantación en forma de plan de acción que la entidad debe encarar para lograr disponer de todos los beneficios que un SGCN ofrece. Entre otros, asegurar la continuidad de los procesos críticos de negocio, teniendo en cuenta los requisitos a los que se ve sometido el mismo.

En los anexos puede encontrarse el detalle de alternativas en cuanto a la implantación de medidas aplicables para afrontar la continuidad de negocio, así como un glosario de términos empleados en la memoria.

En el último capítulo se detallan las referencias bibliográficas, consultadas principalmente para la elaboración de la metodología y citadas a lo largo de la memoria.

2. Metodologia

Para la consecución del proyecto del SGCN se ha seguido la siguiente metodología, que sigue las directrices marcadas por la norma internacional ISO22301 y determina los pasos a seguir para su implantación mediante escalas de medida uniformes y comparables.

Esto permite definir un proceso de gestión de la continuidad de negocio en la entidad común para todas las áreas implicadas y que, ciclo tras ciclo, puede ir incluyendo otros departamentos o localizaciones.

La capacidad de ampliación de alcance en ciclos sucesivos a la implantación es debido a que se tienen en cuenta todos los tipos de activos que pueden participar en los procesos de negocio críticos, ya sean activos IT, proveedores, instalaciones, edificios, personas y ubicaciones técnicas (p.e. Data Centers).

De la misma manera, el hecho de disponer de escalas de medida uniformes y comparables también permite que los resultados sean medibles y equiparables, pudiendo cuantificar la evolución de la entidad en los años tras diversas iteraciones del ciclo de mejora contínua.

2.1 Descripción del proceso de implantación

La implantación de un SGCN basado en ISO22301, se puede dividir en dos facetas claramente diferenciadas:

- Gestión de la continuidad o del propio SGCN
- Operación de la continuidad o del propio SGCN

La primera de ellas tiene una estructura totalmente integrable con el resto de Sistemas de Gestión para los que el órgano internacional emite normas ISO (p.e. calidad, medio ambiente, gestión de riesgos, seguridad informática…) que marcan las directrices de implantación y mantenimiento, de la misma manera que norma en la que se basa el presente proyecto. Esta situación se ha hecho patente en los últimos años, a raíz de las nuevas versiones de los estándares ISO, que permiten a las organizaciones que requieran de la implantación de más de un Sistema de Gestión abordarlas de una manera unificada, con el

consiguiente ahorro de costes que se desprende, y haciendo que la dedicación no se duplique o triplique cuando se decide disponer de más de un Sistema de Gestión. Las secciones de la norma que se incluyen en este ámbito de gestión del propio SGCN son:

- Análisis del Contexto
- Liderazgo
- Planificación
- Soporte
- Evaluación
- Mejora

La segunda faceta hace referencia a los aspectos técnicos más estrechamente relacionados con la continuidad (Operación del SGCN), de la misma manera que en otros Sistemas de Gestión basados en otras normas ISO centran esta sección en las particularidades técnicas de su ámbito de aplicación. La sección de la norma ISO22301 que describe la Operación del SGCN contiene los siguientes ejercicios o actividades:

- Control de la Planificación
- Análisis de Impacto de Negocio
- Análisis de Riesgos
- Estrategias de Continuidad de Negocio
- Establecimiento e implementación de los Procedimientos de Continuidad de Negocio
- Ejercicios y Pruebas

Aunque en el proceso de implantación es recomendable seguir cierto orden de ejecución de tareas, las restricciones temporales o la madurez de la organización en aspectos de continuidad pueden establecer un escenario en el que se combinen en el tiempo acciones o actividades de la vertiente de gestión y de operación del SGCN.

A continuación se describen cada una de las secciones, ejercicios y actividades introducidas en este apartado.

2.1.1.Contexto

Este apartado del SGCN describe los objetivos y las líneas estratégicas además de delimitar los procesos, activos y relaciones con terceros (también conocidos como Partes Interesadas) que forman parte del

mismo, aplicable a los procesos de negocio que se deseen incluir en el alcance.

Debe tenerse en cuenta en esta sección la actividad de negocio de la organización de manera globalizada, sus objetivos esenciales, la tipología de la propia organización, las funciones asignadas, el tipo de servicios que se prestan, las áreas que conforman la organización, análisis de Partes Interesadas y análisis de factores internos o externos que puedan tener una afectación sobre los servicios críticos incluidos en el alcance.

Este apartado se establece al principio de un proyecto de implantación y se erige como punto de partida para todo el análisis de partes interesadas, determinación del alcance y definición de la metodología de mantenimiento y revisión del SGCN, tanto a nivel organizativo como documental.

Adicionalmente, en este apartado se incluyen tanto la definición del criterio y umbral de riesgo, así como el análisis legal y regulatorio al que está sujeta la organización, por el hecho de prestar servicios de atención de llamadas.

2.1.2.Liderazgo

El presente capítulo aborda la definición y asignación de roles, responsabilidades y autorizaciones suficientes para que el SGCN se pueda operar de manera efectiva.

Figura 2.1: Esquema relativo a la organización y liderazgo. VER REFERENCIAS

La asignación de roles a personal de la organización significa cierta dedicación a tareas relacionadas con la operación del SGCN, con lo que la organización debe ser consciente de los costes que ello supone, generalmente traducido en los siguientes aspectos:

- Dedicación de personal a tareas relacionadas con la operación del SGCN (asistencia a reuniones, validación de documentación y material de concienciación y formación, etc.)
- Inversión en mejoras de los activos que soportan los procesos críticos de la organización

Asimismo, la organización que implante un SGCN debe conocer los beneficios que éste supone para la misma que, aun asumiendo los costes descritos anteriormente, suponen un incremento significativo del valor añadido que percibe la organización tanto en el ámbito interno como el externo.

El hecho de comunicar a la organización y establecer un compromiso con la operación del SGCN se hace patente con la definición de la Política de Continuidad, piedra angular del SGCN, y su validación por el máximo órgano de poder de la organización, habitualmente la Dirección General.

Por la importancia para la operación y efectividad del SGCN ésta parte del mismo debe abordarse justo después de haber establecido todos los aspectos analizados en el Contexto. De esta manera se asegura que el personal puede implicarse con la dedicación en el tiempo requerido para la correcta gestión de la continuidad y se empiezan a establecer los criterios de gestión del riesgo del ciclo de mejora PDCA en el que se basa la ISO22301.

2.1.3.Planificación

En esta sección se pretende establecer un tratamiento de los riesgos y las oportunidades que surjan a lo largo de la implantación del SGCN (así como en los siguientes ciclos de mejora continua PDCA) de manera adecuada, teniendo en cuenta su importancia y urgencia de tratamiento.

Tanto las oportunidades como los riesgos indicados deben estar vinculados directamente con los objetivos establecidos en el apartado de Contexto, a la vez que se los esfuerzos se deben concentrar en el alcance establecido en el capítulo de Liderazgo.

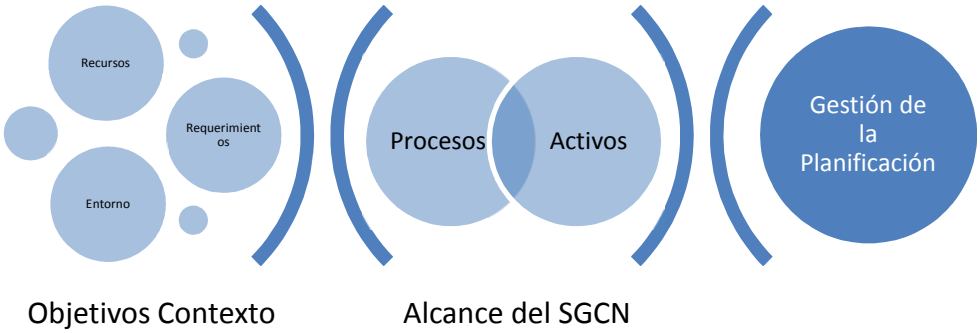

Figura 2.2: Principales variables para gestionar la Planificación. FUENTE PROPIA

Teniendo lo anterior en cuenta, debe acometerse la gestión de Planificación como fase siguiente al establecimiento del Liderazgo del SGCN en la organización. De esta manera se consigue disponer de un control del correcto desarrollo del proyecto, teniendo en cuenta los recursos disponibles y pudiendo analizar las necesidades al contexto y entorno cambiantes a la que la organización y la continuidad de sus procesos críticos de negocio están expuestos.

La mencionada gestión de la Planificación comprende la determinación de acciones concretas (a realizar por personal de la organización

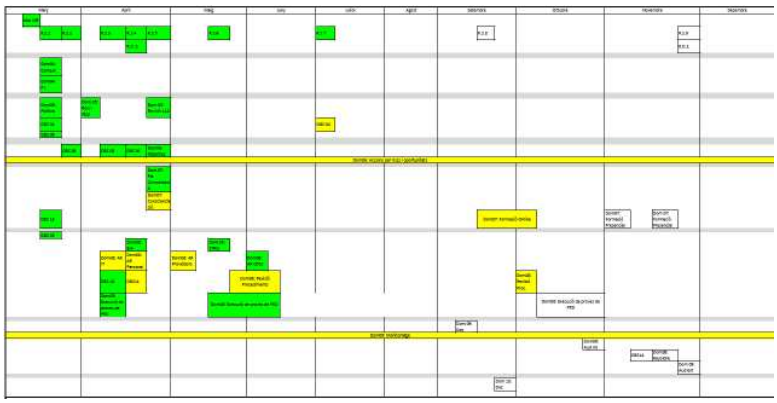

Figura 2.3: Ejemplo de planificación de la implantación de SGCN. FUENTE PROPIA

involucrado en la gestión de la continuidad) relacionadas tanto con las oportunidades a aprovechar y los riesgos a mitigar, como con los objetivos a conseguir.

Los objetivos de continuidad establecidos en la sección de Contexto se analizan aquí para asegurar que se alinean con las directrices marcadas por la organización, ser medibles, satisfacer los requisitos de continuidad y ser actualizados con una periodicidad suficiente.

2.1.4.Soporte

Este apartado del SGCN trata de la determinación de los recursos concretos necesarios para la correcta gestión de la continuidad de los procesos críticos de la organización, el análisis de los requisitos y capacidades de los mismos, incluyendo los roles definidos en la sección de Liderazgo. Asimismo, en este apartado se aborda la metodología de formación y concienciación en lo que se refiere a materia de continuidad que debe estar alineada con los planes de formación y concienciación que ya existan en la organización.

Otro de los más importantes elementos de Soporte para llevar a cabo la gestión de la continuidad de negocio es el análisis y diseño del Plan de Comunicación, que da cabida a todas las fases de continuidad (normalidad, contingencia, crisis, recuperación) y tiene las siguientes variables en la determinación de las acciones de comunicación:

- Tiempo tras el cual realizar la comunicación después de un evento
- Periodicidad de la comunicación
- Contenido de la comunicación
- Canal de comunicación
- Partes Interesadas a las que realizar la comunicación
- Fuentes de información necesarias
- Responsabilidades y autorizaciones vinculadas con el análisis realizado en la fase de Liderazgo.

Adicionalmente, el Soporte incluye la definición de la metodología de gestión documental y el archivado de la información necesaria para la gestión y operación del SGCN.

La implantación de la presente fase no tiene una necesidad de secuencial, como las fases anteriores, de manera que puede combinarse la Planificación de acciones relativas al Soporte junto con acciones encaminadas a las secciones expuestas a continuación. La prioridad y urgencia de dichas acciones debe haberse establecido y verse reflejada en la Planificación establecida en el apartado anterior.

2.1.5.Operación

En este apartado se llevan a cabo los análisis en profundidad, tanto cualitativos como cuantitativos, pruebas técnicas y definición y concreción de las estrategias de continuidad necesarias para preservar los procesos críticos. Dentro del ciclo de PDCA de Deming, enmarcamos el presente apartado en la fase de DO.

Dada la complejidad y amplitud de los análisis necesarios para abordar todos los ejercicios a llevar a cabo en este capítulo es necesario planificar las tareas y actividades relacionadas con el mismo desde las fases más tempranas de la implantación del SGCN. En los siguientes sub-apartados se describen brevemente los ejercicios más significativos a realizar para conseguir los objetivos de la presente sección.

2.1.6.1. Análisis de Riesgos

Este ejercicio establece un proceso análisis a las amenazas y vulnerabilidades a las que están expuestos los procesos de negocio críticos y los activos que los soportan.

Dicho proceso debe quedar adecuadamente documentado para su posterior revisión, adaptación y comparación con la repetición del mismo ejercicio de manera periódica para comprobar que las medidas de salvaguarda aplicadas surten los efectos deseados sobre los riesgos de interrupción de procesos críticos identificados por la organización mediante los sucesivos ciclos de mejora que plantea la norma ISO22301.

Para poder garantizar la repetitividad y valía del ejercicio, éste debe estar basado en una metodología sistemática, que permita priorizar el tratamiento de los riesgos identificados teniendo en cuenta los costes de dichos tratamientos.

Es necesario analizar los procesos críticos de negocio, determinando sus fases, las entradas y salidas de las mismas, los activos que participan

en cada fase así como sus interdependencias. En base a este análisis deben evaluarse cuales son los riesgos reales de interrupción a los que están expuestos los procesos críticos de negocio de la misma manera que la manera de tratarlos, dentro de las posibilidades de la organización y sus objetivos de continuidad teniendo en cuenta el umbral de riesgo determinado en la sección de Contexto.

El resultado del presente ejercicio es un listado de riesgos priorizado según su importancia, teniendo en cuenta la probabilidad de explotación de las vulnerabilidades a las que están expuestas las amenazas existentes, y el impacto que pueda suponer la pérdida de disponibilidad de los activos esenciales para la operación de los procesos críticos de negocio.

2.1.6.2. Análisis de Impacto de Negocio (BIA)

Las tareas relacionadas con el presente sub-apartado (en adelante BIA, de las siglas en inglés: Business Impact Analisys) tienen el objetivo de identificar y cuantificar los activos esenciales para desarrollar los procesos críticos de negocio en un nivel aceptable para la organización, en caso de ocurrencia de una interrupción inesperada en la cadena de suministros.

El BIA debe tener en cuenta las actividades que son necesarias para operar los procesos de negocio críticos, determinando el impacto que supone una interrupción para dicha operación en función del tiempo y definiendo la manera en la que debería recuperarse para asegurar que se cumplen los objetivos de continuidad de negocio fijados en la sección de Contexto.

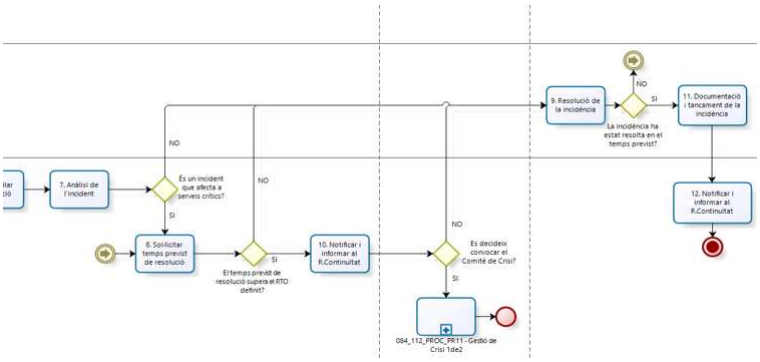

Figura 2.4: Ejemplo de flujo de proceso crítico. FUENTE PROPIA

El impacto de interrupción de las actividades debe ser medible en una escala homogénea, comparable y objetiva en relación a la imagen de la organización frente a sus clientes, competidores y resto de Contexto. De la misma manera debe prestarse atención al impacto económico que

puede suponer las mencionadas interrupciones, así como el posible impacto legal que puedan suponer.

El resultado de este ejercicio es la determinación de los niveles mínimos de operación aceptables de los activos críticos y las actividades que soportan los procesos críticos de negocio, los períodos de tiempo aceptables de interrupción de dichas actividades y la tolerancia en la pérdida de datos permitida, en cualquier caso, con el fin de satisfacer los objetivos de continuidad de negocio.

2.1.6.3. Estrategias de Continuidad de Negocio

Una vez se ha realizado el análisis de riesgos a los que está expuesta la organización, y se conoce el impacto negativo que pueden provocar si estos riesgos se materializan deben definirse las Estrategias de Continuidad. Llegados a este punto se hace necesario disponer de ciertos "escenarios de desastre" que ejemplifiquen de manera generalista los riesgos más significativos a los que está expuesta la organización. Para cada escenario de desastre se deberá escoger una estrategia de continuidad adecuada, para garantizar que los procesos de negocio críticos cumplen con los objetivos de continuidad marcados en la sección de Contexto.

Para ello, primeramente se debe partir de la comparación entre el estado actual de los activos que dan soporte a los procesos críticos de negocio, en cuanto a la redundancia de los mismos, el compromiso de mantenimiento que se tenga con un proveedor, las posibilidades de recuperación en caso de indisponibilidad, el tiempo que se necesita para ello y otros aspectos relacionados con la continuidad frente a los requerimientos que haya fijado el negocio en el sub-apartado del BIA. Para dicha comparación deben tenerse en cuenta las interdependencias entre diferentes partes que deban actuar para recuperar un activo afectado por un incidente, y todos los tipos de activos que den soporte a los procesos de negocio críticos.

Una vez se conoce el estado de satisfacción de los requerimientos de continuidad de negocio por parte de los activos analizados, deben llevarse a cabo dos ejercicios:

I. Plantear una serie de alternativas que permitan que todos los activos puedan cumplir con los objetivos y términos de continuidad fijados anteriormente. Dichas alternativas deben tener en cuenta

todas las posibilidades que ofrezca la tecnología, el mercado y el contexto con el que se relaciona la organización.

II. Determinar a alto nivel las acciones a llevar a cabo en caso de que la organización se vea expuesta de incidente que afecte a la continuidad de sus procesos de negocio críticos. Ejemplos de estas acciones a llevar a cabo podrían ser: Traslado de las oficinas de administración centrales al centro de respaldo, balanceo de los servidores disponibles en alta disponibilidad o activación de acuerdos con organizaciones vecinas.

De entre las alternativas que puedan surgir del primero de los dos ejercicios descritos, debe realizarse un estudio de viabilidad de implantación de las alternativas planteadas con el objetivo que la organización decida la estrategia más adecuada a escoger, teniendo en cuenta el impacto negativo que supondría la no satisfacción de los objetivos de negocio y el coste o inversión que implicaría aplicar una de las alternativas planteadas, que sí permitirían alcanzar los objetivos de continuidad establecidos.

El estudio de las estrategias de negocio debe llevarse a cabo de manera posterior al Análisis de Riesgos y el BIA, descritos en esta misma sección, pues ambos son entradas (o inputs) del presente sub-apartado.

2.1.6.4. Procedimientos de Continuidad de Negocio

En este sub-apartado se detallan cada una de las acciones a llevar a cabo en situaciones como las descritas a continuación, siguiendo las directrices de las Estrategias de Continuidad escogidas por la organización:

- Respuesta a incidentes que afecten a la continuidad de los procesos críticos de negocio
- Gestión de la crisis
- Gestión de la vuelta a la normalidad
- Operación de los procesos de negocio críticos con niveles de degradación aceptables basados en umbrales mínimos de disponibilidad de activos
- Operación de procesos relacionados con la gestión de la continuidad

Deben detallar quien es el responsable de las tareas a llevar a cabo, el tiempo esperado de ejecución de todas ellas, la secuencialidad de las

tareas a llevar a cabo, las comunicaciones a realizar y las decisiones a tomar por el rol autorizado a hacerlo.

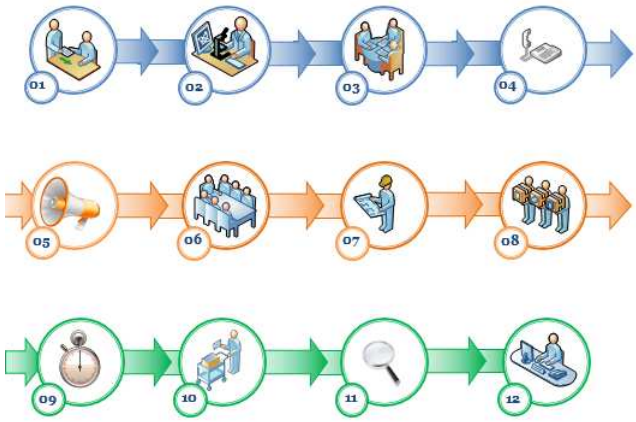

Figura 2.5: Esquema de proceso de gestión de crisis. FUENTE PROPIA

A partir de la información que puede extraerse del análisis realizado en el BIA, deben tenerse en cuenta las interrelaciones entre procesos de negocio y activos que les dan soporte en la definición de los Procedimientos de Continuidad. Estos deben estar enfocados a aprovechar las Estrategias de Continuidad más adecuadas de las que dispone la organización, que consiguen minimizar las consecuencias de las interrupciones de los procesos críticos de negocio con los recursos e inversiones abordables.

La implantación de la presente sub-sección debe abordarse como paso posterior a la determinación de las Estrategias de Continuidad, dada su importancia en el enfoque de todas las tareas de los Procedimientos.

2.1.6.5. Ejercicios y pruebas

La realización de pruebas permite verificar que el SGCN resta actualizado y operativo. Adicionalmente, también permite familiarizar a los empleados clave con los aspectos relacionados con la Gestión de la Continuidad de Negocio (tareas de concienciación y formación) y asegurar que se tienen en cuenta los diferentes escenarios de contingencia definidos por tal de recuperar los procesos de negocio dentro de los términos establecidos en el análisis BIA.

Las pruebas deben verificar que los siguientes puntos se satisfacen:

- Asegurar que el SGCN se adecúa a las necesidades de la organización

- Las personas implicadas en el Plan de Continuidad conocen los detalles del mismo
- Coordinación entre las diferentes Partes Interesadas (grupos o personas) que intervienen
- Correcta ejecución de los diferentes procedimientos del Plan de Continuidad
- Los recursos de infraestructura necesarios están disponibles
- Alineamiento de los procedimientos de recuperación definidos que dan soporte a los procesos de negocio críticos con la realidad de la organización.

Los informes resultantes de las pruebas deben permitir detectar observaciones y desviaciones por tal de registrarlas, revisarlas posteriormente y efectuar un seguimiento efectivo por tal que, finalmente, se traduzcan en la modificación y mejora del Plan de Continuidad de la organización.

Es recomendable llevar a cabo pruebas sobre todos los componente participantes en el alcance del SGCN de forma periódica (p.e.: anual) y después de cambios significativos en cualquier activo que de soporte a los procesos de negocio críticos.

2.1.6.Evaluación

Esta sección describe la manera en la que se deben establecer el conjunto de métricas e indicadores del SGCN y que deben facilitar la toma de decisiones de los órganos de mayor responsabilidad de la organización. Éstas métricas e indicadores deben estar alineados con los objetivos de continuidad establecidos en la sección de Contexto, demostrando la conformidad del SGCN y sus procesos frente a los objetivos de negocio a

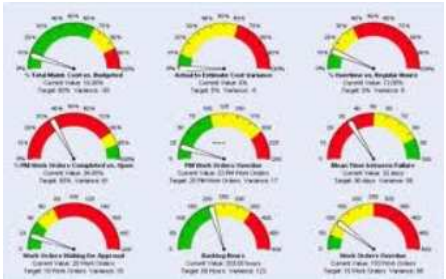

Figura 2.6: Ejemplo de cuadro de mando de indicadores. VER REFERENCIAS

la vez que se mejora la eficacia de los sistemas y activos que le dan soporte. Aunque la definición y medida de las métricas e indicadores no

puede ser abordada desde un primer momento o fase de la implantación del SGCN, esta tarea debe afrontarse de manera secuencialmente posterior a la determinación de los objetivos de negocio de la organización, para poder empezar cuanto antes a medir su evolución y adecuación.

Esto se consigue midiendo y comparando los datos de la operativa habitual relacionados con los resultados, progresos o calidad de la gestión de la continuidad.

El resultado de las métricas e indicadores se deberá reportar de manera periódica a los órganos de gobierno de la organización y revisarse, sobre todo los indicadores que demuestren una evolución negativa o insatisfactoria.

Esta sección también comprende la realización de una Auditoría Interna, que se trata de un ejercicio de validación que debe llevarse a cabo como mínimo una vez dentro de cada ciclo de mejora. El objetivo de dicho ejercicio es validar que el SGCN está alineado con los objetivos de continuidad de la organización y sus requerimientos, así como con los requerimientos fijados por la norma ISO22301, en la que se basa el presente proyecto.

La Auditoria Interna debe revisar todo el alcance definido en el SGCN (determinado en la sección de Liderazgo), basarse en los resultados de las anteriores auditorias, las metodologías utilizadas en la implantación del SGCN y tener en cuenta las competencias, responsabilidades definidas por la organización. La Auditoria Interna debe abordarse en un punto del ciclo de mejora en el que haya suficiente madurez de implantación de los diferentes procesos y procedimientos a tener en cuenta en el SGCN. De esta, manera, se dispone de información suficiente con la que contrastar debidamente los objetivos del ejercicio de la Auditoria Interna.

Finalmente, esta sección también incluye el procedimiento de Revisión por Dirección, o por parte de los órganos de gobiernos competentes en la organización capaces de tomar decisiones sobre los medios económicos y recursos y activos sobre los que se apoyan los procesos de negocio críticos.

La Revisión por Dirección es un proceso necesario dentro del SGCN, por tal de mantener el principio de mejora continua. Con esta revisión se pretende que los órganos de gobierno tengan todo el conocimiento sobre el estado y evolución del SGCN y, si fuera necesario, se tomen las

decisiones necesarias para asegurar la idoneidad, disponibilidad, adecuación y efectividad del mismo. La realización del ejercicio de la Revisión por Dirección puede llevarse a cabo parcialmente en ejercicios dentro del mismo ciclo de mejora, debiendo ser una prioridad desde el inicio del proyecto la validación de los objetivos de continuidad de negocio, así como la evolución de las métricas e indicadores necesarios para alcanzarlos.

2.1.7.Mejora

El presente capítulo detalla cómo tener en cuenta los aspectos que permiten acometer las acciones relacionadas con la mejora continua del SGCN.

El ciclo PDCA en el que se basa la implantación y mantenimiento del SGCN detalla cuatro fases esenciales que deben ejecutarse de manera sistemática para alcanzar la mejora continua. De esta manera, la finalización de la última etapa realimenta a la primera, para volver a repetir nuevamente el ciclo y todas las actividades necesarias para operar el SGCN.

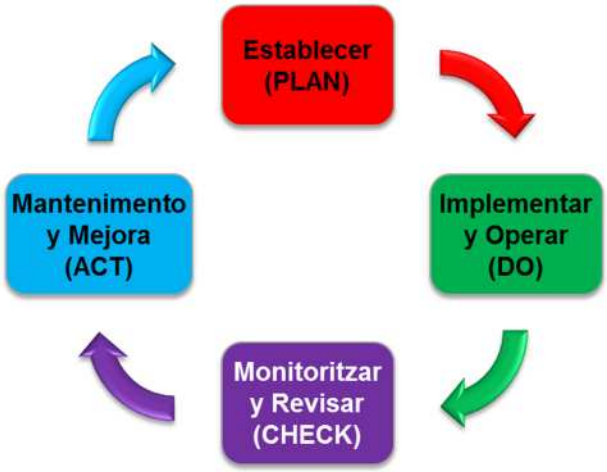

Figura 2.7: Esquema ciclo PDCA (Plan-Do-Check-Act). FUENTE PROPIA

A partir de estas fases se determinan los planes de acción que aseguran la mejora continua, detallándose en acciones correctivas o preventivas, según su origen.

Entre las acciones correctivas a tener en cuenta cabe destacar aquellas que permitan corregir incumplimientos de los controles de los estándares y/o legislación vigente aplicables. Los mencionados incumplimientos pueden ser detectados durante cualquier fase de la implantación del SGCN aunque se debe prestar especial atención a los que se hayan

detectado en las auditorías internas o externas (necesarias para una certificación de la norma ISO22301 por parte de una entidad externa independiente autorizada).

En cambio, las acciones preventivas tienen el objetivo de anticiparse a futuros incumplimientos de la normativa y/o legislación vigente aplicables como desviaciones u omisiones en términos de continuidad que podrían suponer un comportamiento defectuoso del SGCN.

Dada la importancia del ciclo PDCA en el que se basa la norma ISO22301, debe tenerse en cuenta la ejecución de la presente sección desde las fases más tempranas de la implantación del SGCN.

3. Caso Práctico

3.1 Contexto del proyecto

El presente proyecto plantea la implantación sobre cualquier tipo de call center, teniendo en cuenta las siguientes variables como posibilidades de aplicación de la metodología descrita en el capítulo anterior:

- Función del call center dentro de la organización
  - Interno
  - Servicio a terceros
- Tipo de servicio prestado por el call center
  - Acción de marketing
  - Atención al cliente
  - Soporte técnico
  - Llamadas de emergencia
  - Información
- Ámbito del servicio prestado
  - Público
  - Privado
- Volumen de negocio
  - Menos de 10 operadores
  - Entre 10 y 100 operadores
  - Más de 100 operadores

Durante todo el ciclo de implantación debe considerarse como aspecto clave la colaboración de personal interno de la organización responsable de los procesos críticos de negocio vinculados a la prestación de los servicios de call center analizados en el presente proyecto. Esta colaboración se divide en varias fases a lo largo de la implantación del SGCN mediante reuniones, acciones de revisión y validación, así como participación activa en pruebas y auditorías.

A lo largo de las siguientes secciones se describe con orden cronológico el proyecto de implantación de un SGCN siguiendo las directrices de la norma ISO22301 sobre cada uno de sus dominios.

3.2 Alcance

El primer paso a dar para la implantación de un SGCN es delimitar el alcance del mismo en cuanto a procesos de negocio se refiere. En el caso de un call center, deben determinarse primeramente cuáles de los procesos de negocio que ofrece el propio call center deben estar dentro del alcance del SGCN. Para realizar este ejercicio las personas responsables de los procesos de negocio del call center

deben decidir, por su importancia, interdependencia e impacto de la interrupción de los mismos sobre la organización, si todos los procesos de atención de llamadas o parte de ellos serán incluidos en el alcance.

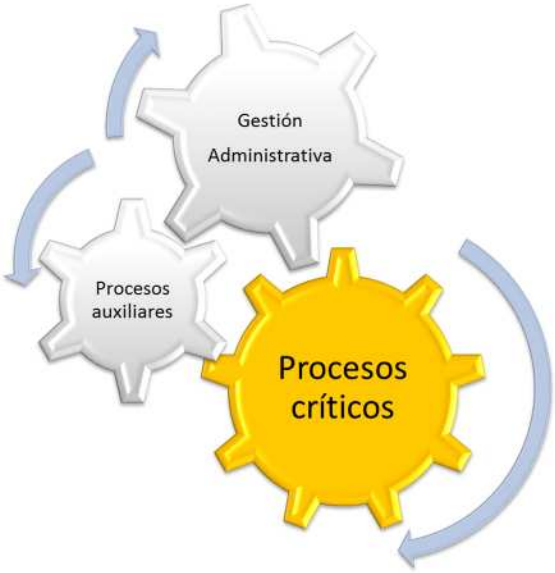

Figura 3.1: Esquema que marca el alcance sobre los Procesos Críticos. FUENTE PROPIA

Una vez seleccionados estos primeros procesos de negocio, debe analizarse la dependencia de los mismos respecto el resto de procesos de negocio de la organización (p.e. administración, compras, ventas, nóminas, gestión de las TIC) para determinar si alguno de ellos (o parte de los mismos) también debe formar parte del alcance del SGCN.

La gestión de los aspectos generales de la organización como son los suministros básicos de electricidad, agua, climatización, los utensilios y maquinaria necesaria para la productividad del puesto de trabajo necesario para el call center son procesos de negocio que siempre deben incluirse en el alcance del SGCN.

Teniendo en cuenta los casos abordados en el presente proyecto, la importancia de incluir diferentes procesos de negocio se puede resumir en la siguiente tabla:

Importancia	Interno	Servicio a terceros
Público	Baja	Media
Privado	Media	Alta

Tabla 3.2: Tabla de importancia en la inclusión de procesos de negocio auxiliares en el alcance del SGCN. FUENTE PROPIA

En la determinación del alcance los call centers que ofrezcan un servicio público de carácter interno (p.e. soporte técnico informático al usuario de una entidad pública gubernamental) la importancia de involucrar a procesos de negocio externos a la propia prestación del servicio es baja, pues su servicio ser podría prestar sin riesgo de interrupción aunque el resto de procesos de negocio de la organización

tuvieran que detener su operación temporalmente. En este caso se podría aproximar que el único evento externo al call center que podría causar la interrupción del servicio prestado sería el cese de la propia organización de manera globalizada.

Como contrapartida, el hecho de prestar un servicio a terceros como organización del ámbito privado, el hecho de no incluir las dependencias del resto de la organización en el alcance podría llegar a suponer un daño en la imagen de la organización, que podría conllevar a pérdidas económicas y competitivas difícilmente subsanables para la organización (en una extensión mucho más amplia si se trata de un call center en el que se basa toda la operación de la organización).

En los casos de un servicio interno en una organización privada y servicio público ofrecido a terceros, debe tenerse en cuenta la inclusión de otros procesos de negocio externos a la prestación del servicio de call center de manera limitada, llegando a plantear ciertas colaboraciones o acuerdos que pueden establecer compromisos en caso de necesidad del servicio de call center.

Cabe destacar que el alcance del SGCN debe ser aprobado por la figura responsable de la organización capaz de decidir cómo se gestionan los recursos del call center y, asimismo, esta figura debe volver a aprobar la determinación del alcance si este se ve modificado dentro del mismo ciclo de mejora o en ciclos posteriores.

3.3 Planificación

Una vez se dispone del alcance sobre el que debe implantarse el SGCN, y en función de las áreas y los responsables de procesos de negocio implicados, se deben establecer reuniones de trabajo y seguimiento para ir abordando los aspectos que recoge la norma ISO22301. El presente apartado no se ve afectado por el tipo de call center analizado, pues la planificación de acciones debe abordarse en cualquier caso de implantación de un SGCN.

El primero de los hitos a tener en cuenta en la planificación es la formalización del compromiso de la dedicación de recursos a la operación del SGCN, pues el personal implicado en ello deberá dedicar parte de su tiempo de trabajo a dar soporte a la implantación. Este soporte suele llevarse a la práctica aportando información necesaria, validando conclusiones y aportando los recursos necesarios para la correcta implantación del SGCN. El compromiso que se debe formalizar debe establecerse con una figura que posea capacidad de decisión sobre los recursos de la organización, o como mínimo, sobre los recursos destinados al call center. Habitualmente se implica a la Dirección de la organización por su poder de decisión en la misma, o el responsable del servicio de call center, en caso de tener un presupuesto propio que pueda destinar a las acciones que considere relevantes y necesarias. La manera de formalizar dicho compromiso se puede evidenciar con

un documento firmado por el promotor del SGCN (Dirección o responsable del servicio), en el que se deje constancia de su entendimiento y conformidad en la dedicación necesaria de los diferentes recursos implicados en la operación del SGCN.

A partir de ese primer hito, deben establecerse (dentro del ciclo de mejora, generalmente anual) todos los pasos a dar hasta terminar la implantación del SGCN. El orden de dichos pasos puede verse ligeramente modificado por aspectos de negocio, como pueden ser, despliegues de nuevo software para la gestión del call center, la previsión de alta dedicación del equipo que da soporte al SGCN por la propia actividad del call center, etc.

Las acciones que deben planificarse inmediatamente después de fijar el alcance y obtener el compromiso de la dedicación de los recursos necesarios son el análisis de contexto del call center y el análisis del impacto de negocio (en adelante BIA), pues después de realizar estos ejercicios cabe la posibilidad de que el alcance sea levemente modificado, por haber descubierto nuevas dependencias con agentes externos o internos al call center. Esto se debe a que el análisis de contexto y el BIA deben llevarse a cabo mediante ejercicios sistemáticos y objetivos.

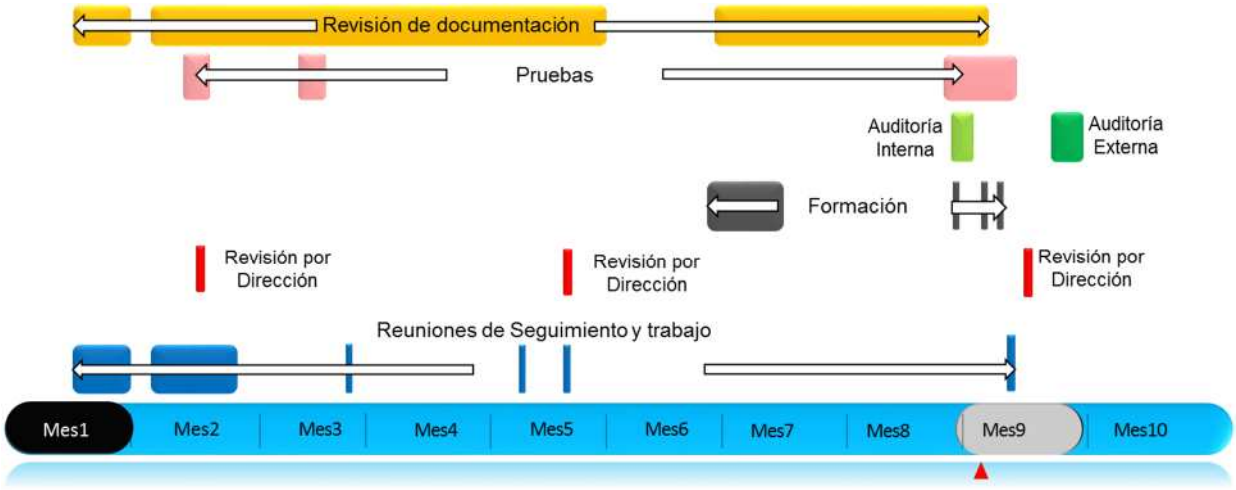

Figura 3.3: Ejemplo de planificación de implantación de SGCN. FUENTE PROPIA

Las siguientes acciones a planificar, dentro del ciclo de mejora del SGCN están relacionadas con la definición de roles dentro del SGCN, sus funciones, responsabilidades y autoridades, la determinación de una política de continuidad y los objetivos estratégicos del call center respecto al servicio que presta. Este punto debe quedar debidamente documentado y aprobado por el promotor del SGCN, pues a partir de dicha formalización, cada rol es asignado a las personas implicadas, de la misma manera que las tareas, responsabilidades y autoridades determinadas. Los objetivos estratégicos, generalmente definidos a alto nivel y con poco nivel de concreción, deben desarrollarse hasta conseguir definir acciones

concretas para alcanzarlos y las métricas e indicadores necesarios para disponer de una visión de la evolución del SGCN sobre su efectividad y adecuación a los requerimientos de la norma ISO22301. El valor de dichas métricas e indicadores se deben revisar de manera periódica en reuniones de seguimiento y presentarse al promotor del proyecto para su validación y toma de decisiones.

A continuación deben planificarse las acciones relativas a los análisis de riesgos a realizar sobre los activos que dan soporte a los procesos de negocio incluidos en el alcance. Estos tienen como objetivo determinar en cuáles de ellos se deben focalizar los recursos destinados a la mejora continua y las acciones de mitigación de los riesgos de continuidad detectados.

Una vez realizados los análisis de riesgos, deben acometerse las acciones relativas a la concienciación y formación para las partes interesadas (internas y externas) con el objetivo de que, sea cual sea la situación a la que se vea expuesto el call center, se realicen las acciones acordadas para asegurar la continuidad de negocio del call center.

Seguidamente se debe analizar si las estrategias de continuidad de negocio que se disponen desde el call center satisfacen los requerimientos establecidos en el BIA. Llegados a este punto, y dada la necesidad de disponer de documentación que dé soporte a los aspectos recogidos en el SGCN, debe reflexionarse los criterios de documentación que deberán aplicarse a toda la documentación del SGCN, para asegurar que todos los documentos tienen un formato homogéneo y se mantienen de la misma manera.

A continuación deben establecerse los planes de continuidad de negocio y procedimientos de recuperación y vuelta a la normalidad de los procesos de negocio incluidos en el alcance del SGCN. Este paso es fundamental para la realización de las pruebas, pues la validez de éstas se comprueba respecto a lo definido en los procedimientos de recuperación y vuelta a la normalidad.

Finalmente se deben definir las acciones a acometer en caso de que alguno de los indicadores presente una evolución negativa, pues esto significaría que se pone en duda que los objetivos estratégicos determinados por el promotor del proyecto puedan alcanzarse. De la misma manera se debe establecer como acometer los aspectos detectados en las auditorías, que denotan ciertas desviaciones respecto los requerimientos que establece la norma ISO22301, en la que se basa el SGCN presentado en el presente proyecto.

Una vez se ha llevado a cabo la planificación de todos estos aspectos, puede determinarse cuando llevar a cabo los ejercicios de auditoría (tanto interna como externa, ésta última en caso que se considere obtener una certificación). La planificación de estos ejercicios debe fijarse cuando el SGCN tenga un grado de implantación suficiente para que la auditoria de unos resultados suficientemente

significativos y válidos para el call center, y por extensión, a la organización. Es decir, si la auditoria se lleva a cabo en una fase demasiado temprana de la implantación, habrá muchos aspectos que no podrán ser evaluados y por tanto la auditoría no podrá aportar un input significativo, como aspecto de mejora continua. Una vez se supera el ciclo de mejora de la implantación (mantenimiento), es recomendable que los ejercicios de auditoria se lleven a cabo de manera distribuida en el tiempo, para que la mejora continua se gestione de forma más prorrateada.

3.4 Compromiso del Promotor

Las acciones que se desprenden de este apartado son necesarias y clave para el éxito de la implantación del SGCN, con el fin de mantener el principio de mejora continua. Dichas acciones tienen el objetivo de que el promotor del SGCN tenga todo el conocimiento necesario sobre el estado y evolución del propio SGCN y, en caso de necesidad, éste pueda tomar las decisiones necesarias para asegurar la idoneidad, disponibilidad, adecuación y efectividad del SGCN. Deben considerarse las acciones descritas en esta sección en cualquier tipo de call center, independientemente de su tipología, función, ámbito y tamaño.

Figura 3.4: Esquema relativo al compromiso del Promotor. VER REFERENCIAS

A continuación se detallan cada uno de los aspectos a trasladar al promotor del SGCN, para formalizar su compromiso con el SGCN, de acuerdo con los requerimientos de la norma ISO22301:

- Alcance del SGCN. Delimita los procesos de negocio, activos y terceras partes implicadas en los que destinar los recursos necesarios para operar el SGCN.
- Roles necesarios para la operación del SGCN. Se deben explicar cada una de las funciones de los roles más significativos, así sus responsabilidades y autoridades, haciendo énfasis en las que recaen sobre el rol del promotor.
- Planificación del SGCN. Una vez fijados dentro del ciclo de mejora todas las acciones descritas en la sección 3.3, el promotor debe aprobarlos para dar conformidad al tiempo que cada uno de los roles definidos debe dedicar a los ejercicios y acciones planificadas.

- Objetivos estratégicos del SGCN. El promotor debe aprobar la estrategia del SGCN, que marca las directrices sobre las cuales se basa toda la operación del propio SGCN. Debe desarrollarse también un método de medición de los mismos que será aprobado también por el promotor en este ejercicio de compromiso.
- Definición de la Política de Continuidad. Se trata de un documento que marca las directrices sobre las que pivota todo el SGCN y es donde el promotor expresa sus intenciones con respecto a la gestión de la continuidad del call center. Es recomendable incluir los objetivos estratégicos en dicho documento, dado lo significativos que resultan para el SGCN. Este documento suele añadirse en las acciones de concienciación y formación para reforzar la importancia de la gestión de la continuidad, así como se hace llegar a las partes implicadas en la misma.
- Metodología de análisis de riesgos y de su tratamiento. El promotor debe aprobar los parámetros determinados para llevar a cabo el análisis de riesgos, los aspectos que se tienen en cuenta y las posibilidades de tratamiento de los riesgos que se detecten como resultado de dicho análisis. Así mismo, debe determinar el umbral de riesgo a partir del cual se debe decidir el tratamiento de los riesgos.

3.5 Análisis de Contexto

Este apartado tiene como objetivo tener en cuenta todos los agentes internos y externos que puedan afectar a la gestión de la continuidad el call center, pudiendo ser éstos muy cambiantes con respecto a las variables enumeradas en la sección 3.1.

Figura 3.5: Esquema relativo al contexto del call center. FUENTE PROPIA

Si tenemos en cuenta la función del call center dentro de la organización, el análisis de contexto se verá muy reducido en el caso de tratarse de un servicio ofrecido de manera interna en la organización, pues su contexto se centra en otras partes de la organización con los que se relacionan para reportar resultados, ofrecer el propio servicio de call center o consumir recursos necesarios para prestar el servicio, como por ejemplo, equipos informáticos, suministros, material de oficina y mobiliario. En el caso de tratarse de un call center que ofrece servicios a terceros externos a la organización el análisis de contexto debe también extenderse a otros ámbitos como los proveedores que participan en la cadena de suministros, los competidores que puedan tener u otras organizaciones que lleven a cabo su operación en la cercanía de la ubicación del call center.

En cuanto a la variable de tipo de servicio prestado por el call center, marcará generalmente el tipo de regulaciones a las que se ve sujeto el servicio prestado, y los requerimientos que éstas fijen en cuanto a la continuidad del propio servicio. Los tipos de servicio que suelen estar más sujetos a regulaciones con requerimientos de continuidad son atención al cliente, llamadas de emergencia e información.

Si tomamos como variable el ámbito, generalmente, el ámbito público está más sujeto a regulaciones y acuerdos con otras organizaciones y entidades. En cambio, el ámbito privado, deberá tener en cuenta, dentro de su análisis de contexto, todos aquellos factores que puedan incurrir en pérdidas económicas, pues su operación siempre estará ligada en mayor o menor medida a la generación de beneficios para la organización.

Por último, el tamaño del call center no influye en el análisis de contexto del mismo, pues los factores internos o externos a los que se vea expuesto el call center respecto a la gestión de la continuidad no dependen del tamaño del mismo.

En cualquier caso, el análisis de contexto debe recoger también los resultados del compromiso del promotor sobre el umbral de riesgo y los criterios de tratamiento del mismo. El umbral de riesgo es el límite de riesgo que la organización está dispuesta a aceptar, sin darle ningún tipo de tratamiento (o implantación de salvaguardas o medidas de mitigación de dichos riesgos). En la siguiente tabla se plantea una posible escala de niveles de riesgos sobre los que decidir su tratamiento y fijar el umbral de riesgo:

Nivel de Riesgo	Descripción
Bajo	Se presupone que no tiene afectación sobre el negocio.
Medio	Es posible que este riesgo tenga una afectación parcial sobre el negocio.
Alto	La materialización de este riesgo comporta una afectación grave sobre el negocio.
Crítico	La materialización de este riesgo comporta una afectación catastrófica

Nivel de Riesgo	Descripción
	sobre el negocio.

Tabla 3.6: Escala de riesgo. FUENTE PROPIA

El coste de conseguir un nivel de riesgo bajo en el call center es muy alto, pues es necesario aplicar muchas medidas de salvaguarda y dedicar muchos recursos, de tal manera que en cuanto a delimitar un cierto umbral de riesgo, hay que tener muy presente el presupuesto económico del que se dispone y las inversiones que podrían llegar a realizarse a corto o medio plazo. Ésta es una de las causas de porqué el promotor debe ser una persona que, dentro de la organización o call center, tenga poder de decisión y conocimiento de los recursos económicos y humanos disponibles a la dedicación de las acciones relacionadas con el SGCN.

Una posibilidad, para fijar el umbral de riesgo puede ser entre los niveles Medio y Alto, lo que significa que los riesgos de nivel Medio y Bajo no recibirían ningún tipo de tratamiento y serían automáticamente aceptados por la organización.

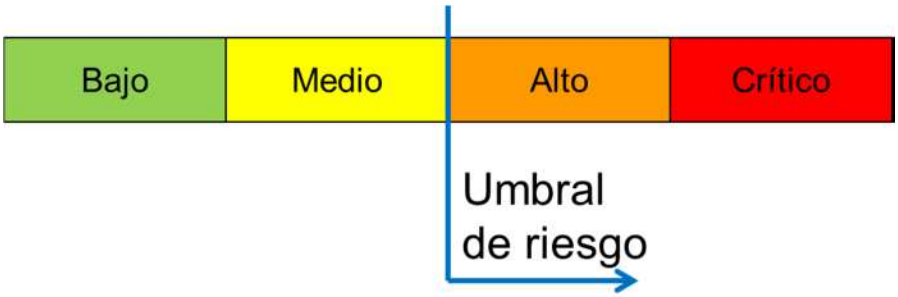

Figura 3.7: Representación gráfica del Umbral de Riesgo. FUENTE PROPIA

En cuanto al tratamiento de los riesgos, deben tenerse en cuenta las siguientes cuatro posibilidades:

I) **Evitar el riesgo**. La manera de evitar el riesgo es eliminar el activo que da soporte a alguno de los procesos de negocio incluidos en el alcance.

II) **Transferir el riesgo**. Cuando la organización se plantea la transferencia de riesgos, debe tener en cuenta la contratación de seguros o llegar a acuerdos con terceras partes para que asuman las consecuencias del riesgo en cuestión.

III) **Mitigar el riesgo**. Esta opción abarca cualquier acción que se realice por parte de la organización que tenga el objetico de aplicar salvaguardas sobre los activos, ya sea para prevenir o detectar vulnerabilidades que puedan ser explotadas o acciones a realizar para corregir las consecuencias de alguna amenaza materializada.

IV) **Aceptar el riesgo**. Esta opción consiste en no llevar a cabo ninguna acción, ni de manera interna a la organización ni de manera externa.

Otro de los aspectos que se debe acometer en el análisis de contexto aplicable para cualquier call center es el análisis de Partes Interesadas. La metodología planteada sigue un modelo que tiene en cuenta tanto elementos internos a la organización (Dirección, óganos de gobierno, asesores, empleados y otras áreas de la organización ajenas al call center) como elementos externos (clientes, proveedores, inversores, reguladores, competidores, familiares del personal, entre otros). Para cada una de las clasificaciones de Partes Interesadas de la siguiente figura, se debe analizar sistemáticamente los requerimientos de continuidad que el call center tiene frente a ellos y detallar concretamente cuáles son esas Partes Interesadas.

Por último, debe también analizarse el marco legal al que está sujeto el servicio que presta el call center, extrayendo de las leyes aplicables cualquier requerimiento de continuidad que pueda afectar al call center, y por extensión a la organización.

3.6 Análisis de Impacto de Negocio

El presente apartado describe la importancia y los aspectos a tener en cuenta en el ejercicio necesario y obligatorio para la implantación de un SGCN. El Análisis de Impacto de Negocio (en adelante BIA, por su acrónimo en inglés) permite identificar cuáles son los procesos esenciales del servicio prestado por el call center, no solamente desde el punto de vista de su valoración estratégica o criticidad, sino también desde el punto de vista del impacto negativo que tiene la interrupción de estos sobre el servicio prestado por el call center.

El impacto negativo de un proceso se evalua en función del tiempo en que dicho proceso no se puede ejecutar obteniéndose un valor máximo de interrupción de los servicios que el negocio está dispuesto a aceptar. Este valor máximo conocido como RTO (Recovery Time Objective) permite determinar el tiempo de recuperación de cualquier proceso y por tanto la estratégica a seguir para recuperarlo.

Cualquier tiempo de recuperación superior a este RTO sería inaceptable para el negocio, hasta llegar al Tiempo Máximo de Parada Tolerable (MTPD-Maximum Tolerable Period of Disruption) que se define como el tiempo máximo que puede estar un proceso o servicio parado sin comportar un impacto catastrófico que provoque daños irreversibles a la organización.

Otra variable a tener en cuenta es el RPO (Recovery Point Objective). El RPO determina el punto (tiempo) desde donde es necesario recuperar la información después de un incidente disruptivo y, por lo tanto, el volumen de datos que la organización tolera perder en el caso que se produzca un escenario de contingencia.

Para realizar el ejercicio del BIA es necesario disponer de la colaboración de personal interno del call center que disponga de una visión transversal o globalizada

del servicio que se presta. De esta manera se asegura que se llegan a determinar los activos y recursos mínimos necesarios para operar el servicio de call center, las interdependencias entre los diferentes procesos de negocio incluidos en el alcance y su dependencia de los diferentes activos necesarios.

Cada uno de los procesos de negocio incluido en el alcance del SGCN debe ser evaluado frente a las siguientes escalas de impacto, según el tiempo avanza desde la ocurrencia de un incidente disruptivo. Se deben tener en cuenta los impactos negativos que puedan afectar a la organización causados por la interrupción del servicio de call center respecto a su imagen, legales, económicos, comerciales y operacionales.

Nivel de Impacto	Descripción
Leve	Afectación entendida y aceptada por los usuarios habituales sin pérdida de confianza en el servicio, aun con los inconvenientes originados.
Medio	Afectación que origina comentarios negativos entre los usuarios habituales del servicio y que comporta pérdida de confianza recuperable en el servicio o aplicación de la organización.
Grave	Afectación importante de la confianza en el servicio por parte de los usuarios y el público en general. Por su gravedad se puede extender y afectar a otras áreas de la organización. La afectación de la confianza es prolongada y puede requerir de aclaraciones y acciones posteriores para la recuperación de la imagen del servicio.
Catastrófico	Afectación que comporta pérdida total de confianza por parte de los clientes, la imagen de la organización queda dañada. Aclarar el incidente o recuperar la imagen requerirá de acciones posteriores, campañas de restauración de la imagen e incluso la comparecencia de la Dirección General o de sus colaboradores directos.

Tabla 3.8: Tabla de niveles de impacto en la imagen. FUENTE PROPIA

Nivel de Impacto	Descripción
Leve	Produce un fallo en el cumplimiento de algún contrato que obliga a renegociar.
Medio	Produce una falta grave en el cumplimiento de algún contrato que comporta responsabilidad legal.
Grave	Deja a la organización al margen de la ley.
Catastrófico	Las autoridades deciden el cese total o parcial de las operaciones de la organización.

Tabla 3.9: Tabla de niveles de impacto legal. FUENTE PROPIA

Nivel de Impacto	Descripción
Leve	< a 10.000 €
Medio	De 10.000 a 60.000 €
Grave	De 60.000 a 150.000 €
Catastrófico	> a 150.000 €

Tabla 3.10: Tabla de niveles de impacto económico. FUENTE PROPIA

Nivel de Impacto	Descripción
Leve	Los clientes del call center no aprecian degradación en el servicio prestado.
Medio	Los clientes aprecian que el servicio prestado por el call center sufre ciertas deficiencias. El negocio generado por el call center se ve reducido durante la influencia del impacto negativo.
Grave	Los competidores del call center detectan la oportunidad de aumentar su cuota de mercado. Así mismo el call center afectado pierde parte de sus clientes.
Catastrófico	La mayoría de los clientes del call center dejan de utilizar los servicios que éste presta.

Tabla 3.11: Tabla de niveles de impacto comercial. FUENTE PROPIA

Impacto operacional:

Nivel de Impacto	Descripción
Leve	Las operaciones del call center se ven reducidas en un 5% o menor.
Medio	Las operaciones del call center se ven reducidas entre un 6% y un 20%
Grave	Las operaciones del call center se ven reducidas entre un 21% y un 50%
Catastrófico	Las operaciones del call center se ven reducidas en un 51% o mayor

Tabla 3.12: Tabla de niveles de impacto operacional. FUENTE PROPIA

Del resultado final se deberá realizar una ponderación, si es necesario, de los valores resultantes en función de la importancia del tipo de impacto. Esta ponderación final depende del tipo de las variables indicadas en la sección 3.1., a continuación se detallan las ponderaciones a realizar para las combinaciones de dichas variables.

En servicios de call center que se presten de manera interna a la organización debe desestimarse el impacto negativo comercial, pues no hay ningún tipo de competidor que ofrezca el mismo servicio. De la misma manera, pierden sentido los impactos relativos a conceptos económicos o legales.

Si tenemos en cuenta call centers que pertenezcan al ámbito público, tampoco debemos darle especial importancia a los impactos comerciales o económicos, pues generalmente, el servicio de call center se presta sin ánimo de lucro y como servicio a la ciudadanía (p.e. información o llamadas de emergencia). Generalmente, los servicios prestados en el ámbito público están más sujetos a regulaciones y leyes, por lo tanto, el impacto legal es significativo en el presente análisis.

En el resto de casos, debe analizarse concretamente con los responsables de negocio las afectaciones particulares que tengan los servicios de call center de los que son responsables.

Una vez se han desestimado los impactos no aplicables al call center se deberán tener en cuenta los requerimientos más restrictivos de cada uno de ellos para

determinar los parámetros resultantes del análisis (RTO, RPO y MTPD entre los más significativos). Para ello se debe evaluar cada uno de los impactos en función del tiempo que haya transcurrido a partir de la ocurrencia de un incidente disruptivo.

Debe tomarse como referencia para la determinación del RTO el tiempo a partir del cual el impacto pasa a ser grave, de modo que se disponga de capacidad de reacción por parte de la organización para recuperarse de las consecuencias acaecidas. La determinación del RPO se calcula de la misma manera que el RTO, aunque teniendo en cuenta el tiempo desde la ocurrencia del incidente disruptivo hacia atrás. En cambio, para la determinación del MTPD, se debe tener como referencia un impacto catastrófico, pues este parámetro indica un límite máximo de interrupción.

Adicionalmente, el análisis BIA debe recoger cualquier tipo de método alternativo para la ejecución de los diferentes procesos de negocio incluidos en el alcance del SGCN, pues éstos permitirían seguir ejecutando la operación del call center para ciertos escenarios de desastre. Uno de los casos más habituales a tener en cuenta como método alternativo en la atención de llamadas es la toma y registro de datos del llamante en formato no digital (en caso de fallo informático en las estaciones de trabajo o en el software que se utilice con ese fin). Claramente el servicio se ve degradado en el caso descrito, pues el tiempo de atención de la llamada se demora y la capacidad del call center se ve disminuida, de manera que también se debe determinar el tiempo máximo en el que se puedan ejecutar los procesos de negocio con estas vías alternativas.

3.7 Liderazgo

En esta sección se definen las principales figuras (en adelante roles del SGCN) o estructuras organizativas en las que se apoya el SGCN y se establecen sus responsabilidades, funciones y autoridades, como base para garantizar la continuidad de los procesos de negocio incluidos en el alcance. Cabe indicar que alguno de los roles ya han sido inicialmente asignados y dotados de algunas de sus principales funciones por el propio lanzamiento del SGCN, como por ejemplo el promotor.

El presente proyecto presenta la estructura organizativa de roles necesarios para operar el SGCN diferenciando entre las fases de la continuidad a las que se ve expuesta cualquier organización:

- Estado de normalidad: Implantación, revisión y mejora continua del SGCN
- Gestión de incidentes: Acciones destinadas a la contención y la respuesta frente incidentes
- Gestión de crisis: Activación y vuelta a la normalidad de los planes de continuidad

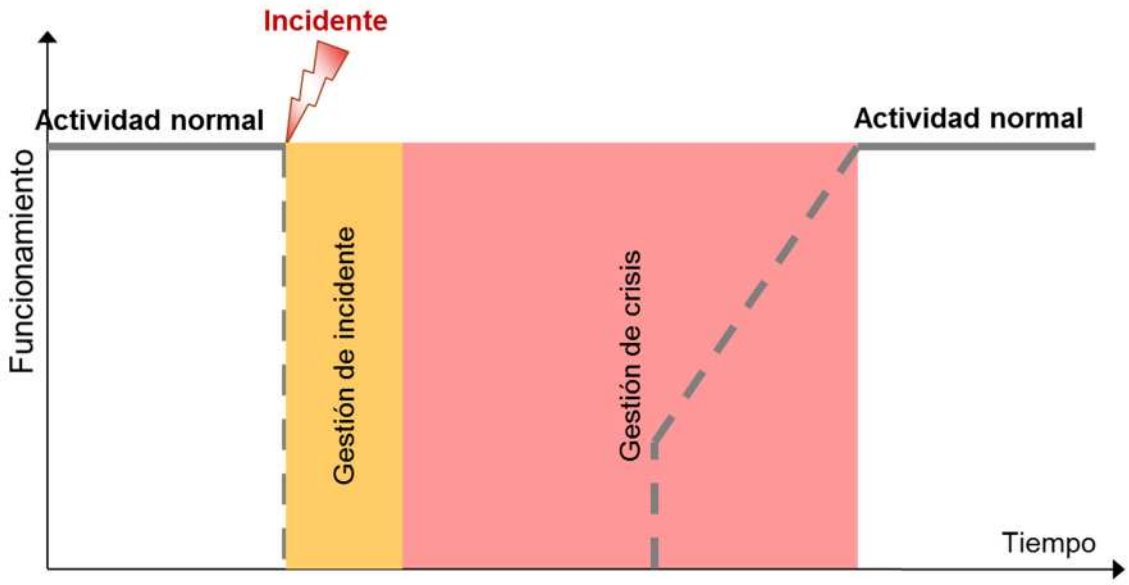

Tabla 3.13: Representación gráfica de las fases de la continuidad de negocio. FUENTE PROPIA

3.7.1. Estado de normalidad

En este estado el call center opera con normalidad los servicios y procesos de negocio incluidos en el alcance del SGCN. Es el estado destinado a realizar las tareas de gestión, implantación y mantenimiento del SGCN, dada la estabilidad de operación del call center en este estado. Dichas tareas se llevan a cabo según las directrices que elabora el Grupo de Trabajo del SGCN. A continuación se enumeran sus funciones principales:

- Tratar los aspectos de continuidad de negocio en las reuniones de órganos de gobierno (p.e. Consejos de Dirección) de la organización como un proceso clave para la misma
- Dar soporte y dotar de recursos a los equipos de personas involucradas en la continuidad de negocio
- Designar roles que deben gestionarla continuidad de negocio
- Definir la política, normativa y objetivos en materia de continuidad, alineados con la estrategia de la organización
- Dar aprobación al a documentación del SGCN y los cambios en la misma.
- Participación en la formación, pruebas y mantenimiento del plan de continuidad
- Transmitir la importancia de la gestión eficaz del SGCN y promover la mejora continua
- Participar en las reuniones de revisión por dirección (promotor) y aprobar las acciones correctivas o preventivas del plan de acción
- Determinar el nivel de riesgo aceptable en la organización y aceptar los riesgos que excedan ese nivel, si fuera necesario

- Asegurar que se realizan auditorías internas y que el SGCN consiguen los resultados esperados

El siguiente esquema muestra los roles que componen el equipo de continuidad, para dar satisfacción a todos los requerimientos marcados por la norma ISO22301. Cabe indicar que no es necesario que cada rol sea asignado a personas diferentes, aunque si recomendable. Finalmente, el tamaño del call center determinará cuantas personas pueden asignarse a cada rol.

Equipo de Continuidad				
Promotor				
Gestor Continuidad de Negocio				
Gestor incidentes	Responsable Área TIC Área TIC	Responsable Operaciones Área Operaciones	Responsable Prueba Auditor Prueba	Responsable RRHH
Asesor SGCN	Auditor Interno		Auditor Externo	

Tabla 3.14: Tabla de roles involucrados en estado de normalidad. FUENTE PROPIA

A continuación se detallan las responsabilidades y autoridades de cada uno de los roles que forman parte del Equipo de Continuidad.

PROMOTOR
RESPONSABILIDADES
• Participación activa en los ejercicios más significativos dentro del ciclo de mejora continua (reuniones trimestrales, formaciones, auditorías, pruebas) • Proponer acciones correctivas y/o preventivas si los resultados no son los esperados, velando por la implantación del SGCN • Designar el resto de roles y recursos necesarios para el buen funcionamiento del SGCN de acuerdo a los requerimientos de experiencia y formación para formar parte del Equipo de continuidad.
AUTORIDADES
• Aprobación y firma de la Política de Continuidad • Divulgación de información a medios de comunicación, en caso necesario • Validar el cumplimiento de leyes y regulaciones y notificarlas a las Partes Interesadas afectadas por ellas • Aprobar la metodología de medida y seguimiento de la efectividad del SGCN • Criterio y Umbral de Riesgo • Estrategias de continuidad

• Tareas del plan de acción que requieran de su aprobación. Generalmente vinculadas a tratamiento de riesgos que superan el Umbral de Riesgo.

Tabla 3.15: Tabla de responsabilidades y autoridades del Promotor. FUENTE PROPIA

GESTOR CONTINUIDAD DE NEGOCIO
RESPONSABILIDADES
• Gestión de la convocatoria y el liderazgo de las reuniones de Equipo de Continuidad • Ejecución de la formación y pruebas de continuidad • Velar por la actualización y mejora continua del SGCN • Aprobación final de la documentación perteneciente al SGCN, excepto la Política de Continuidad • Determinar un responsable del seguimiento de las acciones de mejora • Distribuir la información sobre continuidad de negocio a los empleados del call center • Designar los responsables de las pruebas de continuidad y definir los objetivos de las mismas • Realizar reuniones de conclusiones de pruebas con sus participantes
AUTORIDADES
• Aprobación de las acciones de mejora que no requieran una validación por parte del Promotor • Aprobar los resultados del BIA (RTO, RPO, MBCO…) • Aprobación de los cambios a llevar a cabo en la documentación • Aprobación del plan de pruebas

Tabla 3.16: Tabla de responsabilidades y autoridades del Gestor de Continuidad de Negocio. FUENTE PROPIA

GESTOR DE INCIDENTES
RESPONSABILIDADES
• Analizar, respecto a los RTO definidos para cada proceso de negocio, el tiempo previsto de resolución de la incidencia • Presentar y analizar los incidentes más importantes en las reuniones del Equipo de continuidad
AUTORIDADES
• Ejecución y mantenimiento del procedimiento de gestión de incidentes • Aprobar el equipamiento y preparación del área de trabajo de apoyo • Validar los datos necesarios a proporcionar para calcular las métricas e indicadores.

Tabla 3.17: Tabla de responsabilidades y autoridades del Gestor de Incidentes. FUENTE PROPIA

EQUIPO DE GESTIÓN DE INCIDENTES
RESPONSABILIDADES
• Ejecución del procedimiento de gestión de incidentes • Mantener actualizados los registros de incidentes • Equipar y mantener preparada el área de trabajo de apoyo • Proporcionar los datos necesarios para realizar los cálculos de las métricas e indicadores • Notificar al gestor de incidentes de cualquier incidencia detectada
AUTORIDADES
-

Tabla 3.18: Tabla de responsabilidades y autoridades del Equipo de Gestión de Incidentes. FUENTE PROPIA

RESPONSABLE ÁREA TIC
RESPONSABILIDADES
• Estar informado de la ejecución de pruebas de continuidad definidas dentro del SGCN • Asegurar la actualización de la documentación del SGCN contiene información correcta sobre los Sistemas de Información • Participar en la definición de las métricas e indicadores
AUTORIDADES
• Validar el buen funcionamiento de los equipos informáticos y software del call center • Validar el equipamiento técnico mínimo del área de trabajo de apoyo • Validar la gestión técnica de la continuidad de negocio, realizando las peticiones de recursos necesarios al Promotor, si fuera necesario

Tabla 3.19: Tabla de responsabilidades y autoridades del Responsable del Área TIC. FUENTE PROPIA

ÁREA TIC
RESPONSABILIDADES
• Responsable que la información del SGCN esté disponible y actualizada en las ubicaciones virtuales determinadas para su almacenamiento • Asegurar el buen funcionamiento de los equipos informáticos y software del call center • Equipar técnicamente y mantener preparada el área de trabajo de apoyo • Gestión técnica de la continuidad, revisando e identificando los recursos materiales necesarios y comunicándolo con el Responsable del Área TIC
AUTORIDADES
-

Tabla 3.20: Tabla de responsabilidades y autoridades del Área TIC. FUENTE PROPIA

RESPONSABLE OPERACIONES
RESPONSABILIDADES
• Notificar al gestor de continuidad los cambios en los procesos de negocio que puedan afectar al SGCN • Detectar necesidades de formación y concienciación en los equipos de trabajo que participan en la ejecución de los procesos de negocio • Participar en el BIA, proporcionando información sobre los procesos analizados
AUTORIDADES
• Validar la correcta ejecución de las actividades pertenecientes a los procesos críticos

Tabla 3.21: Tabla de responsabilidades y autoridades del Responsable de Operaciones. FUENTE PROPIA

RESPONSABLE DE LA PRUEBA
RESPONSABILIDADES
• Comunicar a los participantes de la prueba el lugar y fecha en los que se llevará a cabo • Obtener la aprobación de la guía de la prueba por parte del gestor de continuidad
AUTORIDADES
• Validar el escenario en el que se desarrollará la prueba, su planificación y los objetivos a cubrir • Validar las actividades que se ejecutan durante la prueba y cualquier desviación detectada • Validar el informe de prueba a presentar al resto del equipo de continuidad

Tabla 3.22: Tabla de responsabilidades y autoridades del Responsable de la Prueba. FUENTE PROPIA

RESPONSABLE RECURSOS HUMANOS
RESPONSABILIDADES
• Identificar cambios en el personal que participa en las diferentes fases del SGCN • Participar en la definición del procedimiento de evacuación de las oficinas • Revisar que las pruebas de evacuación del edificio se realizan de manera efectiva
AUTORIDADES
-

Tabla 3.23: Tabla de responsabilidades y autoridades del Responsable de Recursos Humanos. FUENTE PROPIA

ASESOR SGCN
RESPONSABILIDADES
• Definir el escenario de las pruebas de continuidad y evaluar las incidencias y desviaciones detectadas en las mismas • Registrar las conclusiones de las pruebas • Asesorar a otros roles en las tareas a realizar • Generar y mantener la documentación del SGCN • Verificar la correcta ejecución de las tareas registradas en la planificación del SGCN
AUTORIDADES
-

Tabla 3.24: Tabla de responsabilidades y autoridades del Asesor SGCN. FUENTE PROPIA

AUDITOR INTERNO
RESPONSABILIDADES
• Elaboración de un plan de auditoria anual • Generación del programa de entrevistas y organización de las mismas • Realización de la Auditoria Interna • Generar el informe que detalle las no conformidades, observaciones y desviaciones que se hayan detectado durante la auditoria interna
AUTORIDADES
-

Tabla 3.25: Tabla de responsabilidades y autoridades del Auditor Interno. FUENTE PROPIA

AUDITOR PRUEBA
RESPONSABILIDADES
• Realizar seguimiento de todas las actividades desarrolladas durante la prueba y comprobar que están recogidas en la guía de la prueba • Disponer de la guía de la prueba • Analizar las desviaciones detectadas respecto la planificación y comunicarlas al gestor de continuidad, facilitando toda la documentación generada
AUTORIDADES
-

Tabla 3.26: Tabla de responsabilidades y autoridades del Auditor de la Prueba. FUENTE PROPIA

3.7.2. Gestión de incidentes

En el presente apartado se identifican los roles que participan en la fase de gestión de incidentes, con el objetivo de garantizar el correcto tratamiento de la

incidencia y evitar que pueda acontecer una causa mayor al call center que pueda obligar a activar la gestión de la crisis. En el siguiente esquema se enumeran los diferentes roles que participan en la presente fase de la continuidad, para los que seguidamente se describen sus responsabilidades y autoridades.

Gestor de incidentes		
Servicios Generales		
Responsable Área TIC	Responsable Operaciones	Responsable RRHH
Área TIC	Área Operaciones	
Empleados del call center i Colaboradores		

Tabla 3.27: Tabla de roles involucrados en la gestión de incidentes. FUENTE PROPIA

GESTOR DE INCIDENTES
RESPONSABILIDADES
• Liderar el ciclo de vida de los incidentes que puedan producirse • Actuar como punto central de la gestión del incidente en la recolección de datos de los especialistas cada área de negocio • Evaluar los daños y alcance del incidente • Velar por la integridad física de los empleados externos y colaboradores del call center • En caso de evaluar un tiempo de resolución del incidente superior al RTO, notificarlo al Gestor de Continuidad
AUTORIDADES
• Aprobar las medidas iniciales a aplicar para limitar la afectación del incidente • Validar la información recogida por cada área de negocio • Validar el análisis, registro, tiempo de resolución previsto y gestión de la solución del incidente a partir de la información proporcionada

Tabla 3.28: Tabla de responsabilidades y autoridades del Gestor de Incidentes. FUENTE PROPIA

SERVICIOS GENERALES
RESPONSABILIDADES
• Reportar al gestor de incidentes las afectaciones causadas por los incidentes en las instalaciones del edificio desde el que se presta el servicio de call center • Asegurar la seguridad y orden de las instalaciones del edificio desde el que se presta el servicio de call center y de sus componentes internos
AUTORIDADES
-

Tabla 3.29: Tabla de responsabilidades y autoridades de Servicios Generales. FUENTE PROPIA

RESPONSABLE ÁREA TIC
RESPONSABILIDADES
• Realizar las acciones oportunas frente incidentes con afectación a empleados externos y colaboradores pertenecientes al área TIC • Coordinarse con el gestor de incidentes en las acciones a realizar para dar respuesta a incidentes
AUTORIDADES
• Validar la información a notificar al gestor de incidentes de la situación detectada en los sistemas de información • Validar la resolución de incidencias en las estaciones de trabajo • Validar la estimación del tiempo de recuperación del incidente detectado • Autorizar las medidas iniciales para limitar la afectación del incidente

Tabla 3.30: Tabla de responsabilidades y autoridades del Área TIC. FUENTE PROPIA

ÁREA TIC
RESPONSABILIDADES
• Informar y notificar al gestor de incidentes de la situación detectada en los sistemas de información • Resolver las incidencias acaecidas en las estaciones de trabajo • Aplicar medidas iniciales para limitar la afectación del incidente • Revisar permanentemente la evolución del incidente e informar de manera periódica al Gestor de Incidentes • Dar soporte al Gestor de Incidentes a evaluar la afectación de los procesos críticos, si es necesario • Estimar el tiempo de recuperación previsto del incidente detectado
AUTORIDADES
-

Tabla 3.31: Tabla de responsabilidades y autoridades del Área TIC. FUENTE PROPIA

RESPONSABLE DE RECURSOS HUMANOS
RESPONSABILIDADES
• Realizar las acciones oportunas para hacer frente a incidentes con afectación a personal del call center de manera coordinada con el gestor de incidentes • Velar por la integridad física de los empleados del call center • Notificar a las familias de los empleados si éstos han sido afectados por un incidente
AUTORIDADES
-

Tabla 3.32: Tabla de responsabilidades y autoridades del Responsable de Recursos Humanos. FUENTE PROPIA

RESPONSABLE ÁREA DE OPERACIONES
RESPONSABILIDADES
• Realizar las acciones oportunas frente incidentes con afectación a empleados externos y colaboradores pertenecientes al área de operaciones • Coordinarse con el gestor de incidentes en las acciones a realizar para dar respuesta a incidentes
AUTORIDADES
• Validar la información a notificar al gestor de incidentes de la situación detectada en las operaciones del call center • Validar la resolución de incidencias en las estaciones de trabajo • Validar la estimación del tiempo de recuperación del incidente detectado • Autorizar las medidas iniciales para limitar la afectación del incidente

Tabla 3.33: Tabla de responsabilidades y autoridades del Responsable de Operaciones. FUENTE PROPIA

ÁREA DE OPERACIONES
RESPONSABILIDADES
• Informar y notificar al gestor de incidentes de la situación detectada en las operaciones del call center • Aplicar las medidas iniciales para limitar la afectación del incidente • Revisar permanentemente la evolución del incidente e informar de manera periódica al Gestor de Incidentes • Dar soporte al Gestor de Incidentes a evaluar la afectación de los procesos críticos, si es necesario • Estimar el tiempo de recuperación previsto del incidente detectado
AUTORIDADES
-

Tabla 3.34: Tabla de responsabilidades y autoridades del Área de Operaciones. FUENTE PROPIA

EMPLEADOS DEL CALL CENTER Y COLABORADORES
RESPONSABILIDADES
• Detectar y notificar los incidentes detectados al Gestor de Incidentes
AUTORIDADES
-

Tabla 3.35: Tabla de responsabilidades y autoridades de los empleados del call center y colaboradores. FUENTE PROPIA

3.7.3. Gestión de crisis

En el presente apartado se identifican los roles que participan en la parte de operación del plan de continuidad, contemplando su activación y ejecución de los procedimientos de recuperación con el objetivo de restaurar la actividad de los procesos de negocio críticos.

Asimismo, el grupo de trabajo de crisis, o Comité de Crisis, interactúa con otras áreas de la organización para tomar decisiones y activar o delegar acciones. A continuación se enumeran sus funciones principales:

- Revisar y validar la información sobre el impacto del incidente
- Recopilar información y realizar la evaluación final del alcance del impacto del incidente
- Decide la necesidad de activar el plan de continuidad y los procedimientos a ejecutar
- Activar los procedimientos escogidos y convocar al personal adecuado
- Controlar y hacer seguimiento de que los procesos críticos se restauran dentro del tiempo objetivo establecido (RTO)
- Analizar y tomar decisiones sobre los problemas detectados
- Analizar el estado de la organización y, si se considera adecuado, activar el plan de retorno, supervisando las tareas hasta la vuelta a la situación normal, antes de la ocurrencia del incidente

Seguidamente se detallan las áreas que forman el equipo de operación del plan de continuidad (Comité de Crisis).

Comité de Crisis			
Promotor			Áreas De Soporte
Gestor Continuidad de Negocio			
Gestor incidentes	Responsable Área TIC	Responsable Operaciones	
	Área TIC	Área Operaciones	
Puestos de Trabajo Críticos	Áreas de apoyo	Servicios Generales	
Autoridades Pertinentes	Proveedores de Servicios		

Tabla 3.36: Tabla de roles involucrados en la gestión de la crisis. FUENTE PROPIA

PROMOTOR
RESPONSABILIDADES
• Apoyo e implicación que permitan el correcto desarrollo de la continuidad de negocio
AUTORIDADES
• Evaluar la información que le reporta el Comité de Crisis y aprobar o denegar las propuestas • Ser consultado por el Comité de Crisis antes de tomar decisiones importantes en materia de continuidad • Aprobar la priorización de acciones de recuperación • Autorizar la notificación sobre la situación actual a: o Empleados de la organización o Responsables de comunicación de la organización o Medios de comunicación o Otros organismos

Tabla 3.37: Tabla de responsabilidades y autoridades del Promotor. FUENTE PROPIA

GESTOR DE LA CONTINUIDAD
RESPONSABILIDADES
• Convocar al Comité de Crisis si se cumplen los criterios determinados después de analizar el incidente, actuando como punto de contacto con el Promotor • Una vez resuelta la incidencia y restaurados los recursos originales, volver a convocar el Comité de Crisis para iniciar el plan de retorno a la normalidad • Coordinar las acciones de los procedimientos de recuperación y de retorno a la normalidad
AUTORIDADES
• Aprobar y realizar la notificación a proveedores con personal en las instalaciones del call center sobre la situación actual • Validar la ejecución de los procedimientos de recuperación y de retorno a la normalidad • Evaluar las responsabilidades de la organización por las consecuencias de la contingencia (posibles reclamaciones, indemnizaciones, litigios, etc) • Aprobar acciones de compra urgentes de material necesario para la recuperación

Tabla 3.38: Tabla de responsabilidades y autoridades del Gestor de la Continuidad. FUENTE PROPIA

GESTOR DE INCIDENTES
RESPONSABILIDADES
• Asistir al Gestor de Continuidad en todo aquello que le pida e informar al Responsable de Operaciones • Ejecutar o hacer que se ejecuten las acciones que decida el Comité de Crisis • Ejecutar los procedimientos de recuperación y vuelta a la normalidad
AUTORIDADES
-

Tabla 3.39: Tabla de responsabilidades y autoridades del Gestor de Incidentes. FUENTE PROPIA

RESPONSABLE ÁREA TIC
RESPONSABILIDADES
-
AUTORIDADES
• Validar la habilitación de la funcionalidad del área alternativa de trabajo, si se dispone de ella • Validar la recuperación de los sistemas • Validar la ejecución de los procedimientos de recuperación y vuelta a la normalidad • Validar la ejecución de las acciones tecnológicas que determine el Comité de Crisis

Tabla 3.40: Tabla de responsabilidades y autoridades del Responsable del Área TIC. FUENTE PROPIA

ÁREA TIC
RESPONSABILIDADES
• Informar y reportar de forma continua al Gestor de Continuidad • Asesorar al Comité de Crisis en todos los aspectos tecnológicos • Ejecutar o hacer que se ejecuten las acciones relacionadas con la informática y la tecnología determinadas por el Comité de Crisis, ya sean para recuperar o volver a la normalidad
AUTORIDADES
-

Tabla 3.41: Tabla de responsabilidades y autoridades del Área TIC. FUENTE PROPIA

RESPONSABLE DE OPERACIONES
RESPONSABILIDADES
• Asegurar la habilitación de la funcionalidad del área de trabajo alternativa, si se dispone de ella • Asegurar la recuperación de las operaciones y de los procedimientos de recuperación y vuelta a la normalidad
AUTORIDADES
• Validar la ejecución de las acciones operativas que determine el Comité de Crisis

Tabla 3.42: Tabla de responsabilidades y autoridades del Responsable de Operaciones. FUENTE PROPIA

ÁREA DE OPERACIONES
RESPONSABILIDADES
• Informar y reportar de forma continua al Gestor de Continuidad • Asesorar al Comité de Crisis en todos los aspectos operativos • Ejecutar o hacer que se ejecuten las acciones relacionadas con la operación determinadas por el Comité de Crisis, ya sean para recuperar o volver a la normalidad
AUTORIDADES
-

Tabla 3.43: Tabla de responsabilidades y autoridades del Área de Operaciones. FUENTE PROPIA

ÁREAS DE APOYO[1]
RESPONSABILIDADES
• Evaluar las responsabilidades de la organización frente consecuencias de la contingencia (reclamaciones, indemnizaciones, litigios, etc) • Ejecutar acciones de compra urgentes de material necesario para la recuperación • Proveer al área de trabajo de material de oficina • Recoger información necesaria, incluyendo fotos y otro tipo de evidencias, para posibles reclamaciones a las compañías de seguros implicadas • Coordinación de las acciones que impacten sobre el personal de la organización
AUTORIDADES
-

Tabla 3.44: Tabla de responsabilidades y autoridades de las Áreas de Apoyo. FUENTE PROPIA

[1] Las áreas de apoyo en un SGCN pueden identificarse por el área de RRHH, administración, finanzas o asesoría legal y jurídica

RESPONSABLE DE COMUNICACIÓN
RESPONSABILIDADES
• Ejercer como punto único de divulgación de información a terceras partes (ciudadanía, medios de comunicación, otras organizaciones) • Notificar sobre la situación actual de contingencia a: o Empleados de la organización o Medios de comunicación o Otros organismos
AUTORIDADES
-

Tabla 3.45: Tabla de responsabilidades y autoridades del Responsable de Comunicación. FUENTE PROPIA

AUTORIDADES PERTINENTES[2]
RESPONSABILIDADES
• Prestación de servicios de emergencia: urgencias sanitarias, extinción de incendios, salvamento, seguridad ciudadana, protección civil, etc • Actuar en función de la contingencia dando apoyo a la organización, tanto a personal como a edificios e instalaciones
AUTORIDADES
-

Tabla 3.46: Tabla de responsabilidades y autoridades de las Autoridades Pertinentes. FUENTE PROPIA

PROVEEDORES DE SERVICIOS
RESPONSABILIDADES
• Provisión de luz, agua, mantenimiento de equipos técnicos, mantenimiento de las oficinas y el material que las compone • Ejecución de los procedimientos de recuperación • Registrar los cambios que se realicen sobre sistemas o plataformas • Cumplir con los SLA (Acuerdos de Nivel de Servicios, por sus siglas en inglés) contratados y revisión del estado de sus propios Planes de Continuidad • Determinar los posibles problemas de capacidad o disponibilidad que presenten las plataformas de confingencia
AUTORIDADES
-

Tabla 3.47: Tabla de responsabilidades y autoridades de Proveedores de Servicio. FUENTE PROPIA

[2] Las áreas de apoyo en un SGCN pueden identificarse por el área de RRHH, administración, finanzas o asesoría legal y jurídica

PUESTOS DE TRABAJO CRÍTICOS[3]
RESPONSABILIDADES
• Ejecución de las actividades críticas de negocio con los niveles determinados en las condiciones alternativas de trabajo.
AUTORIDADES
-

Tabla 3.48: Tabla de responsabilidades y autoridades de los Puestos de Trabajo Críticos. FUENTE PROPIA

RESPONSABLE DE SERVICIOS GENERALES
RESPONSABILIDADES
• Ejecutar o hacer que se ejecuten las acciones operativas que decida el Comité de Crisis • Participar en la coordinación de las acciones a llevar a cabo si la afectación es a nivel de edificio
AUTORIDADES
• Validar las actuaciones sobre edificios e infraestructuras, y los elementos que los ocupan

Tabla 3.49: Tabla de responsabilidades y autoridades de Servicios Generales. FUENTE PROPIA

3.8 Política de Continuidad y Objetivos Estratégicos

El presente capítulo establece las directrices sobre las cuales deben alinearse todas las acciones preventivas o correctivas detectadas en cualquier fase del ciclo de mejora continua, así como el resto de plan de acción y ejercicios a llevar a cabo con el fin de la implantación o mantenimiento del SGCN.

La Política de Continuidad se establece como piedra angular de la formalización y determinación de las medidas organizativas, logísticas y administrativas previstas para garantizar los procesos de negocio críticos para el call center en el supuesto que una causa de fuerza mayor impidiese proveer dichos procesos desde las dependencias habituales de operación. Al tratarse de un documento tan significativo, éste debe ser aprobado directamente por el Promotor del SGCN.

Se trata de un documento que debe ser tratado como público a nivel interno en la organización, e incluso puede ser publicado al exterior, si se considera conveniente. Esta última opción es la escogida por las organizaciones que implantan SGCN para

[3] Está formado por personas cuyas funciones son indispensables para la realización de los procesos de negocio críticos.

disponer de la ventaja competitiva y de imagen que supone el conocimiento de dicho hito para los clientes o usuarios que reciben los servicios prestados por el call center, en especial si finalmente el SGCN es certificado por una entidad externa independiente. Por tratarse de un documento de tan baja confidencialidad, no es recomendable incluir información confidencial para la operación, continuidad y seguridad del call center, aunque deben describirse brevemente sus funciones principales.

Se debe incluir una mención al alcance del SGCN dentro de la Política de continuidad, así como a sus limitaciones, con el fin de describir concretamente las fronteras de las acciones a acometer para implantar y mantener el SGCN en su ciclo de mejora continua. Entre la descripción de los criterios ejecutivos a reflejar en la Política de Continuidad deben tenerse en cuenta las regulaciones y leyes a las que se ven sujetos los procesos críticos del call center.

Los objetivos estratégicos del SGCN deben también quedar reflejados en la Política de Continuidad, dada su importancia para el mismo, así como para su implantación y mejora continua. Dichos objetivos deben ser desarrollados hasta llegar a definir tareas concretas que consigan el éxito de los objetivos definidos. Dentro de los objetivos estratégicos del SGCN debe incluirse la priorización de acciones para asegurar la protección y seguridad del personal, pues se deja constancia del mismo en la propia norma ISO22301, en la que se basa el presente proyecto. Es aconsejable incluir entre los objetivos estratégicos, el hecho de minimizar la interrupción de las operaciones (o procesos) críticas de negocio, así como la efectividad del Plan de Continuidad, compuesto por todos los procedimientos de recuperación y vuelta a la normalidad necesarios. Aunque es necesario revisar los objetivos estratégicos de manera periódica (en cada ciclo de mejora, como mínimo), estos no deberían verse modificados muy a menudo, pues la estrategia de una organización se establece a medio o largo plazo.

3.9 Análisis de Riesgos

La presente sección describe la manera en la que se lleva a cabo y en qué ejercicios se divide el Análisis de Riesgos al que deben someterse los procesos de negocio incluidos en el alcance del SGCN.

El primero de los ejercicios es aplicar la metodología Magerit de Análisis de Riesgos. Esta tiene como base realizar un inventario de activos que dan soporte a la operación de los procesos de negocio críticos, incluyendo las siguientes tipologías:

- Personal
- Proveedores
- Activos TIC
- Instalaciones y edificios

Debe asignarse un valor a cada uno de los activos recogidos en el inventario, teniendo en cuenta la siguiente escala:

Confidencialidad		Integridad		Disponibilidad	
Nivel	**Descripción**	**Nivel**	**Descripción**	**Nivel**	**Descripción**
1	**Público**	**1**	**Bajo**	**1**	**No crítico**
	Sin restricciones de difusión		La información errónea se puede corregir fácilmente a partir de otras fuentes.		Puede recuperarse en más de diversas jornadas laborales
2	**Uso interno**	**2**	**Normal**	**2**	**Sensible**
	Información que debe tutelarse dentro de la organización, disponible para los operadores del call center		La información errónea se puede corregir a partir de otras fuentes y el esfuerzo para conseguirlo no es excesivo		Debe recuperarse en menos de una jornada laboral. Existen procedimientos alternativos
3	**Restringido**	**3**	**Alto**	**3**	**Crítico**
	Información que debe tutelarse dentro de la organización		La información errónea se puede corregir a partir de otras fuentes y el esfuerzo para conseguirlo es considerable		Debe recuperarse en menos de 2 horas
4	**Confidencial**	**4**	**Molt alt**	**4**	**Vital**
	Información de alta sensibilidad por el impacto en la reputación, potencial de fraude o requisitos		La información errónea es difícil de corregir y tiene un coste alto		Debe recuperarse en minutos

Confidencialidad		Integridad		Disponibilidad	
Nivel	**Descripción**	**Nivel**	**Descripción**	**Nivel**	**Descripción**
	legales				
5	**Secreto** Su difusión puede afectar muy gravemente la actividad del call center	**5**	**Vital** La información no se puede volver a obtener	**5**	**Sin tolerancia a fallos** Debe tener disponibilidad 24 horas al día, todos los días del año

Tabla 3.50: Tabla de escala de valoración de activos. FUENTE PROPIA

Después de asignar uno de estos niveles de valoración a cada uno de los activos del inventario, se debe decidir la ponderación que tendrá cada dimensión (integridad, confidencialidad y disponibilidad) para calcular el valor final de cada activo. Cabe destacar que, en caso de tener pesos diferentes para cada dimensión evaluada, en un SGCN, debe tenerse en cuenta siempre una ponderación mayor o igual que el resto para la disponibilidad.

Seguidamente se debe determinar el conjunto de amenazas que pueden afectar a la continuidad de los procesos críticos de negocio, asignando a cada una de ellas una probabilidad de ocurrencia, que se puede medir mediante la siguiente escala:

PROBABILIDAD	DEFINICIÓN
Poco Frecuente (1-2)	Acontecimiento poco probable que podría experimentarse cada varios años
Normal (3)	Acontecimiento probable que podría experimentarse una vez al año
Frecuente (4)	Acontecimiento muy probable que se experimenta habitualmente una vez al mes
Muy Frecuente (5)	Acontecimiento muy probable que se experimenta frecuentemente, al menos diariamente

Tabla 3.51: Tabla de probabilidad de ocurrencia de las amenazas. FUENTE PROPIA

El conjunto de amenazas determinado conforma el catálogo de amenazas del SGCN, que debe ser validado por el Promotor del SGCN y pueden tenerse como base los siguientes ejemplos y tipologías:

- Desastres Naturales
  - Incendio
  - Inundación
  - Terremoto
- Desastres Internos
  - Incendio
  - Contaminación electromagnética
  - Interrupción del suministro eléctrico
  - Interrupción de las comunicaciones
- Errores no intencionados
  - Errores de usuarios de los sistemas informáticos
  - Errores de mantenimiento
  - Indisponibilidad de personal
- Ataques intencionados
  - Manipulación de configuración
  - Fraude/Suplantación de identidad
  - Ataque destructivo

La interacción de las amenazas descritas ante los activos que dan soporte a los procesos críticos del call center se lleva a cabo a través de la explotación de las vulnerabilidades que dichos activos tienen de manera intrínseca, siendo estas agrupables por los tipos de activo que se tienen en cuenta en el análisis. En la siguiente tabla se detallan algunos ejemplos de dichas vulnerabilidades:

Tipo de Activo	Vulnerabilidad
Instalaciones y edificios	Imposibilidad de acceso
	Ubicación no disponible
	Fallo en el control de acceso físico
Personal	Absentismo
	Falta de concienciación en continuidad
	Falta de capacitación para operar los procesos críticos
Activos TIC	Almacenamiento inadecuado
	Falta de mantenimiento
	Capacidad insuficiente
	Protección inadecuada frente a cambios
	Configuración errónea
	Errores en el control de acceso lógico
Proveedores	Fallo en la provisión del servicio
	Falta de concienciación en continuidad
	Degradación del servicio prestado al call center

Tabla 3.52: Tabla de vulnerabilidades. FUENTE PROPIA

Debe cuantificarse el impacto de cada una de las vulnerabilidades incluidas en el Análisis de Riesgos sobre los activos que dan soporte a los procesos críticos de negocio, dada su posible explotación, siguiendo la escala presentada en la siguiente tabla:

IMPACTO	DEFINICIÓN
Bajo (1-2)	Cierta pérdida de disponibilidad del activo debido a una degradación leve del mismo
Medio (3)	Considerable pérdida de disponibilidad del activo debido a una seria degradación del mismo
Alto (4-5)	Grave pérdida de disponibilidad del activo debido a una degradación muy severa del mismo

Tabla 3.53: Tabla de escala de impacto. FUENTE PROPIA

Una vez asignado el nivel de impacto las vulnerabilidades que puedan afectar a cada tipo de activo, debe establecerse una relación entre las amenazas y las vulnerabilidades, de manera que se puedan cruzar el grupo de vulnerabilidades incluidas en el análisis con las amenazas que las puedan explotar concretamente, y que tengan cierto sentido. Analizando los ejemplos dados deberían cruzarse, como caso ilustrativo la vulnerabilidad de “Errores en el control del acceso lógico” con la amenaza de “Fraude/Suplantación de identidad”. En el *anexo 5.1* se puede ver el cruce completo de las vulnerabilidades y amenazas descritas en el presente capítulo.

Por último, solo falta determinar el nivel de riesgo que se asigna a cada combinación de activo, vulnerabilidad y amenaza que la explota, que puede calcularse con la siguiente fórmula:

$$Riesgo = \begin{pmatrix} Valor\ del \\ activo \end{pmatrix} * \begin{pmatrix} Probabilidad\ de \\ ocurrencia\ de \\ la\ amenaza \end{pmatrix} * \begin{pmatrix} Impacto\ de \\ explotar\ la \\ vulnerabilidad \end{pmatrix}$$

Tabla 3.54: Fórmula de cálculo del Riesgo. FUENTE PROPIA

Seguidamente debe establecerse una escala según la cual asignar los diferentes niveles de Riesgo a cada uno de los casos resultantes del Análisis. Teniendo en cuenta las diferentes combinaciones numéricas posibles al realizar el anterior cálculo, la escala de riesgos se puede establecer de la siguiente manera:

NIVEL DE RIESGO	VALORES
Bajo	1 - 19
Medio	20 - 39
Alto	40 - 59
Crítico	60 - 125

Tabla 3.55: Tabla de niveles de riesgo. FUENTE PROPIA

Con el desarrollo de todos los cruces posibles y su cuantificación y clasificación por nivel de riesgo, el Análisis de Riesgos siguiendo la metodología Magerit se finaliza consiguiendo así el riesgo inherente de los activos. Para conocer el riesgo real (o residual) deben conocerse las medidas de mitigación que el call center o la organización tienen en su operativa habitual, de manera que algunos de los riesgos detectados puedan bajarse de nivel, o incluso ser eliminados.

Es posible realizar otros Análisis de Riesgos complementarios para que la visión que tiene el call center sobre los procesos de negocio que se incluyen en el alcance sea más completa, teniendo en cuenta otras metodologías, aunque debe tenerse en cuenta que todos ellos deben llegar a resultados con la misma escala de riesgo definida anteriormente, para poder ser comparables y priorizar debidamente las acciones que se desprendan. Aunque no se desarrollan en el presente proyecto, pueden tenerse como metodologías complementarias la realización de una evaluación de cumplimiento del marco de controles que marca la ISO27002, que abarca la seguridad de la información sobre las mismas tipologías de activos que la norma en la que se basa el SGCN presentado, así como la evaluación de cumplimiento del marco de controles de la norma TIA-942, que mide cuanto de bien están preparadas las instalaciones informáticas y Centros de Procesado de Datos para prestar un servicio al call center o la organización con ciertos niveles de disponibilidad.

Una vez terminados los ejercicios que se consideren necesarios en cuanto a la realización del Análisis de Riesgos del SGCN, es necesario ordenarlos según su nivel de criticidad, teniendo más prioridad de tratamiento los más críticos, siempre y cuando superen el umbral de riesgo determinado. Para la totalidad de los riesgos que superen este umbral, será necesario registrarlos en el plan de acción para su debido seguimiento.

3.10 Concienciación y formación

Este capítulo describe las acciones a acometer para asegurar que los recursos humanos que dan soporte al SGCN tienen los conocimientos y habilidades necesarias para que puedan ejercer sus funciones en el mismo en cualquiera de las fases de continuidad en la que se encuentre el call center con eficacia y eficiencia. Por tanto, la formación y concienciación tienen como fin el dotar de buena preparación a los todos los roles que participan en el SGCN para que puedan aplicar los conocimientos adquiridos y conseguir así los resultados previstos.

Se considera al rol de Gestor de Continuidad como máximo responsable de la formación de todas las partes interesadas del SGCN, buscando conseguir los siguientes hitos, frente al personal designado para el resto de roles:

- Cumplimiento de las competencias requeridas por cada rol del SGCN
- Mejora de sus habilidades dentro del SGCN
- Tener conocimiento de la existencia del plan de formación y sus objetivo
- Saber quiénes son los roles responsables y los métodos para contactar con ellos
- Conocer los procedimientos del plan de continuidad: activación, recuperación y retorno a la normalidad
- Conocer sus responsabilidades particulares
- Saber que el SGCN no es un plan estático, sino que se realiza mantenimiento en el que deben contribuir

Una buena capacitación del personal requiere, en primer lugar, la evaluación de las necesidades del call center. Una vez se conocen estas necesidades, se identificaran cuáles son los objetivos de formación a proporcionar al personal implicado con el SGCN, se establecerá el temario, así como escoger los medios de formación y el material más adecuados para realizarla (documentación, actividades, duración, periodicidad…).

Figura 3.56: Esquema de formación. VER REFERENCIAS

Finalmente, se llevarán a cabo las sesiones de formación de acuerdo con la planificación establecida, siendo recomendable requerir a los participantes de la formación de la cumplimentación de cuestionarios de calidad sobre su satisfacción en cuanto a la información recibida, ponentes que hayan impartido la formación, contenido, metodología utilizada y adecuación del formato de la formación, entre otros.

Los resultados de la formación deben quedar debidamente registrados para asegurar que todo el personal requerido ha participado en las formaciones consideradas necesarias para su rol dentro del SGCN, así como disponer de información adecuada para poder evaluar las capacidades de los roles. Estos resultados deben ser reportados al promotor del SGCN, para que pueda evaluar su eficacia, identificar puntos de mejora y decidir cuáles son las acciones a realizar por tal de mejorar las capacidades del personal que desarrolla las funciones de todos los roles del SGCN.

El plan de formación debe tener en cuenta el análisis de competencias y las necesidades del personal implicado con el SGCN, especificando las áreas del call center que deben recibir cada formación, el material necesario para realizarlas, el medio y la ubicación en donde llevarlas a cabo y los ejercicios de evaluación a realizar.

En cuanto a la concienciación del SGCN para las partes interesadas y roles determinados, consiste en hacerlos conocedores del SGCN de tal manera que éstos contribuyan a un mejor rendimiento y una mayor eficacia del mismo. Adicionalmente, estas acciones deben hacer foco en reforzar los conocimientos sobre la Política de Continuidad, las implicaciones de un incumplimiento de los requisitos del SGCN y sus funciones durante un incidente disruptivo o desastre. La concienciación siempre debe acompañarse de mensajes que apoyen la bondad del SGCN frente a cualquier contingencia para asegurar la resiliencia y continuidad de los procesos críticos del call center.

Las acciones y ejercicios en los que se hace palpable la concienciación del SGCN pueden dividir entre sesiones presenciales realizadas con cierta periodicidad dentro de cada ciclo de mejora del SGCN y comunicados internos o externos llevados a cabo por los roles adecuados.

Entre las sesiones presenciales cabe destacar las reuniones de seguimiento, de las que su periodicidad depende de la dedicación acordada para los roles participantes en las mismas, atendiendo a los recursos dedicados al SGCN por el promotor. Estas reuniones deben incluir el seguimiento de las tareas y acciones desarrolladas en el análisis de contexto del call center, detallando su grado de avance, así como los resultados de las pruebas que se vayan realizando, revisión de documentación del SGCN, indicadores y métricas, identificación de las partes

interesadas del SGCN sobre las que hacer foco en las acciones de concienciación, y cualquier otro aspecto relevante de interés para la continuidad del call center.

Los comunicados internos o externos a llevar a cabo en relación a concienciación deben ser analizados para asegurar que consiguen los objetivos marcados. Para ello, inicialmente se deben conocer los puntos sobre el SGCN que necesitan refuerzo, para cada una de las partes interesadas o roles del SGCN para, a partir de esto, escoger la temática más adecuada a tratar. La distribución de la acción de concienciación debe acompañarse de la Política de Continuidad por el medio que se considere más adecuado (correo electrónico, mensajería interna, publicación de noticia en página web interna…). También tienen cabida como comunicados internos o externos el emplazamiento de paneles informativos con información clave en puntos visibles desde los puestos de trabajo desde los que se desempeñan los procesos de negocio críticos, o cualquier otra localización dentro o fuera de la organización que se considere adecuado.

3.11 Estrategias de continuidad

La presente sección establece las estrategias a ejecutar en caso de identificar cualquiera de los escenarios de contingencia que afecten de alguna manera a los procesos críticos del call center, con el objetivo de recuperar los servicios prestados en dependencia de los activos afectados en cada caso. Es necesario tener en cuenta los requerimientos temporales establecidos en el análisis BIA para valorar la adecuación de las diferentes estrategias de continuidad que se puedan plantear, en función de los recursos al alcance del call center.

El análisis de las estrategias de continuidad debe contemplar los elementos que intervienen en los siguientes puntos:

a) La existencia de procesos alternativos a los procesos críticos incluidos en el alcance del SGCN, tanto existentes en la actualidad como de posible implantación. El presente punto puede determinarse como toma de datos en formularios de papel en lugar de utilizar los aplicativos necesarios para operar los procesos críticos por posible fallo del sistema, o tener a disponible en un tiempo razonable un entorno con una versión estable de dichos aplicativos anterior a la desplegada en el entorno productivo de operación de los procesos críticos.
b) La organización de los empleados esenciales para mantener los procesos críticos operativos en situación de contingencia de acuerdo a los requerimientos de continuidad de cada proceso. En el caso de que se prestara el servicio de una manera distribuida en dos localizaciones diferenciadas, podría considerarse a todo el personal de la localización no afectada como personal esencial, prestando los procesos críticos de forma degradada al 50% de su capacidad habitual. En este punto deben considerarse las condiciones contractuales con el

personal que presta el servicio para que, en situaciones de contingencia excepcionales, tengan flexibilidad en prolongar su jornada laboral para evitar una pérdida de degradación inaceptable, o realización de guardias por posibles necesidades de refuerzo puntual de personal. En caso algún empleado esencial tenga un perfil único frente al resto de componentes de empleados esenciales (habitualmente vinculado a operación de activos TIC), debe buscarse personal de substitución con unas capacidades y habilidades para desempeñar las funciones de su rol de SGCN equivalentes al empleado esencial de perfil único.

c) Las instalaciones desde las que se desarrollan los procesos críticos, así como áreas de trabajo y centro de procesado de datos[4] (CPD). En este punto se debe tener en cuenta las posibilidades de las que dispone el call center en cuanto a ocupación de otras zonas de la organización, ubicaciones alternativas en otra sede de la organización o acuerdos con otras organizaciones que puedan acoger temporalmente la operación del call center. En cuanto a la infraestructura de CPD, si la organización no dispone de recursos suficientes para disponer de unas instalaciones redundadas en una ubicación no expuesta a las mismas amenazas de manera simultánea debe analizarse la posibilidad de contratar servicios de externalización del CPD o almacenamiento en el Cloud.
d) La información que no se puede perder y el tiempo para su recuperación. Deben analizarse las estrategias disponibles respecto al parámetro RPO, fijado en el BIA, para la información necesaria para operar los procesos críticos de negocio teniendo en cuenta la variabilidad de las mismas. El resultado de este tipo de análisis de estrategia conlleva a fijar la política de ejecución, retención y disposición de las copias de seguridad[5] de la información.
e) Las partes interesadas implicadas en la operación de los procesos críticos. Aquí deben identificarse los proveedores y otras partes de la organización o de colaboradores dentro o fuera del call center que puedan tener que intervenir en la recuperación y operación habitual del call center, los niveles de servicio acordados, los tiempos de resolución de incidentes contratados y la colaboración en general en cualquier fase de la continuidad de negocio relativa al SGCN.
f) Los activos tecnológicos necesarios para mantener los procesos críticos operativos. Debe establecerse de qué manera se va a llevar a cabo la recuperación de cada activo implicado, incluso estableciendo acuerdos en la prestación del servicio con los proveedores que los mantienen y analizando si es necesario disponer de activos tecnológicos en alta disponibilidad (operación balanceada).

[4] Ver en el anexo 5.2 las posibilidades sobre estrategias de recuperación de CPD
[5] Ver en el anexo 5.3 las posibilidades de estrategias en la realización de copias de seguridad

3.12 Planes y procedimientos de continuidad de negocio

Los planes y procedimientos del SGCN pretenden servir como guía documental para la ejecución de las tareas relacionadas con la contención y gestión de los incidentes que ocurran, los desastres en los que se puedan convertir y la recuperación de los procesos críticos de negocio, dadas las consecuencias de un desastre para el call center.

El procedimiento de gestión de incidentes permite la gestión y tratamiento iniciales de cualquier incidencia que pueda afectar la continuidad del call center. A partir de este procedimiento se desencadenan todas las tareas y acciones necesarias para contención y resolución de incidentes, se analiza y evalúa su alcance y afectación respecto los procesos críticos, se realiza las comunicaciones de escalado definidas y, en caso de ser necesario, se activa el Comté de Crisis. Es recomendable disponer de un orden establecido en la activación (o convocatoria) del Comité de Crisis, por ejemplo, siguiendo un árbol de llamadas o mensajería en un medio de comunicación independiente de la operación de los procesos de negocio incluidos en el alcance del SGCN. Dentro del análisis del alcance y afectación, se debe priorizar el conocimiento del tiempo previsto de resolución y las implicaciones para operar los procesos de negocio críticos con normalidad o una degradación tolerada.

Una vez se determina que el incidente cumple con alguno de los escenarios de crisis definidos, deben seguirse las directrices y acciones determinadas en el procedimiento de gestión de crisis con el objetivo de recuperar los procesos de negocio críticos a un nivel aceptable. De forma paralela debe activarse el plan de comunicación del SGCN para coordinar las acciones y tareas necesarias conjuntamente con las partes interesadas implicadas. Puede dividirse el procedimiento de gestión de crisis en dos fases diferenciadas:

a) Activación de la Crisis: Se contempla la activación del Comité de Crisis para el tratamiento inicial del desastre, se recopila la información relativa al mismo, se toman las decisiones necesarias para establecer los procedimientos de recuperación a ejecutar, así como se piden las autorizaciones necesarias para poderlos ejecutar, si fuera necesario.
b) Gestión de la Crisis: Se contempla en esta fase el seguimiento de las acciones determinadas para recuperar un nivel aceptable de la operación de los procesos de negocio críticos (dados los procedimientos de recuperación escogidos), realizando acciones de comunicación con las partes interesadas de manera periódica hasta la resolución del desastre. También en esta fase el Comité de Crisis debe decidir cuáles

serán los procedimientos de retorno a la normalidad y cuando deben ser ejecutados.

Los procedimientos de recuperación tienen que tener en cuenta los activos que participan en los procesos de negocio críticos, cubriendo todos los escenarios de desastre identificados, y con un detalle suficiente como para que el personal designado a los roles que participan en la recuperación puedan ejecutar los procedimientos de manera eficiente y efectiva. Algunos procedimientos a tener en cuenta para recuperar los procesos críticos de un call center son:

- Desvío de llamadas
- Refuerzo de personal
- Traslado de personal
- Activación de ubicación alternativa de trabajo
- Evacuación de las oficinas
- Fallo en el suministro eléctico
- Fallo en la climatización del CPD
- Fallo en la realización/recepción de llamadas
- Fallo del software necesario
- Fallo de comunicaciones de datos (no telefónicos)

3.13 Pruebas

Este capítulo describe como se deben llevar a cabo las pruebas de recuperación de desastres, necesarias para evaluar la bondad y efectividad del SGCN para hacer frente a las incidencias que pueden afectar al call center. Adicionalmente, permite familiarizar a los empleados y partes interesadas participantes en los aspectos relacionados con la continuidad de negocio. Los tipos de pruebas a llevar a cabo se estructuran en diferentes niveles, con un impacto creciente en la organización y el uso de recursos, que trata de garantizar la cobertura de todos los escenarios contemplados en el SGCN. Las pruebas deben verificar que se le da cumplimiento a los siguientes puntos:

- Asegurar que el SGCN se adecúa a las necesidades del call center
- Las personas implicadas en la continuidad conocen suficientemente el detalle del SGCN
- Coordinación entre las diferentes partes interesadas
- Correcta ejecución de los diferentes procedimientos del plan de continuidad

- Alineamiento de los procedimientos de recuperación definidos que den apoyo a los procesos críticos del call center

Los informes resultantes de las pruebas deben permitir observaciones y no conformidades que para ser registradas, revisadas y permitir hacer un seguimiento con el objetivo de la mejora continua del SGCN. Es recomendable realizar pruebas de todos los componentes del plan de continuidad de manera anual, aunque cabe la posibilidad de realizar una planificación durante más de un ciclo de mejora del SGCN. En la realización de pruebas siempre se tiene que evaluar el riesgo de interrupción que supone para los procesos de negocio críticos que se ponen a prueba, debiendo minimizar éste. En la siguiente tabla se pueden ver los diferentes tipos de pruebas a realizar por el call center, dentro del alcance del SGCN, descritas seguidamente:

Prueba de revisión	Pruebas parciales	Prueba total
• **Tipo A:** Revisión "en despacho" de los procedimientos del Plan de Continuidad (en papel).	• **Tipo B:** Simulacro de corte de comunicaciones • **Tipo C:** Recuperación de un elemento técnico del CPD (servidor, switch, etc.) • **Tipo D:** Recuperación del área de trabajo	• **Tipo E:** Se simula una situación de emergencia real

Tabla 3.57: Tabla tipos de pruebas. FUENTE PROPIA

Prueba de revisión

Esta prueba consiste en revisar los procedimientos del plan de continuidad que se precisen evaluar. Parte de la definición de un escenario de desastre teórico para validar que los procedimientos escogidos se ejecutarían de manera correcta, en un caso real. Este tipo de prueba permite comprobar que los flujos de información entre los diferentes participantes son adecuados y que se podría resolver el incidente. Seguidamente se listan los resultados deseados de la prueba de revisión:

- Conocimiento de los flujos de decisiones del plan de continuidad
- Conocimiento de los procedimientos del plan
- Conocimiento de las responsabilidades de cada rol
- Conocimiento de las notificaciones internas en caso de incidente
- Conocimiento de los árboles de llamadas definidos
- Conocimiento de las personas de sustitución
- Conocimiento de recursos alternativos
- Conocimiento de los tiempos asignados a cada fase

Pruebas parciales

Se incluye en estas pruebas validaciones parciales de la operativa global donde se desarrolla una simulación de interrupción de una parte de las infraestructuras contempladas en el plan de continuidad. La ejecución de estas pruebas es necesaria antes de afrontar una prueba total y pueden suponer el único tipo de pruebas a realizar si la prueba total no puede realizarse por tener un riesgo inaceptable de interrupción de los procesos críticos del call center. Seguidamente se listan los resultados deseados de las pruebas parciales:

- Validar la correcta ejecución de los procedimientos de recuperación
- Validar que los procedimientos de recuperación se pueden ejecutar en el tiempo esperado
- Validar que los recursos alternativos pueden operar los procesos críticos con normalidad y sin degradación

Prueba total

En una prueba total se simula una situación de emergencia real donde se puede implicar a toda la organización, empresas externas e incluso servicios de emergencias. Durante estos ejercicios, se llega a interrumpir los procesos críticos de negocio de forma temporal. Con la ejecución de este tipo de pruebas se persigue:

- Validar que el área de trabajo alternativa (en caso de existir) se puede activar con el material necesario para operar los procesos críticos de negocio
- Los tiempos de activación satisfacen el tiempo objetivo esperado
- Los procedimientos de recuperación se ejecutan de manera efectiva y en el tiempo esperado
- Los sistemas informáticos se recuperan correctamente en el CPD alternativo (en caso de existir) en el tiempo esperado

Finalmente, en cualquier tipo de prueba que se lleve a cabo, debe asegurarse que se registra cualquier evento acaecido inesperado que pueda producir una desviación del procedimiento de recuperación testeado, o una dilatación del tiempo de ejecución del mismo. De esta manera, se puede hacer un correcto tratamiento dichos eventos, actualizando la documentación del SGCN, y llevando a cabo las tareas necesarias para corregir las situaciones desfavorables detectadas y aportar así a la mejora continua del ciclo PDCA.

3.14 Evaluación del SGCN

La presente sección trata sobre como tener conocimiento y las herramientas necesarias para tener la certeza de la correcta operación del SGCN y tomar las decisiones oportunas en caso de detectar una tendencia que ponga en riesgo la efectividad del SGCN

A continuación se presenta el modelo para medir y evaluar la bondad de las acciones establecidas para conseguir los objetivos estratégicos, así como detectar las posibles desviaciones que se puedan producir durante cada ciclo de mejora del SGCN:

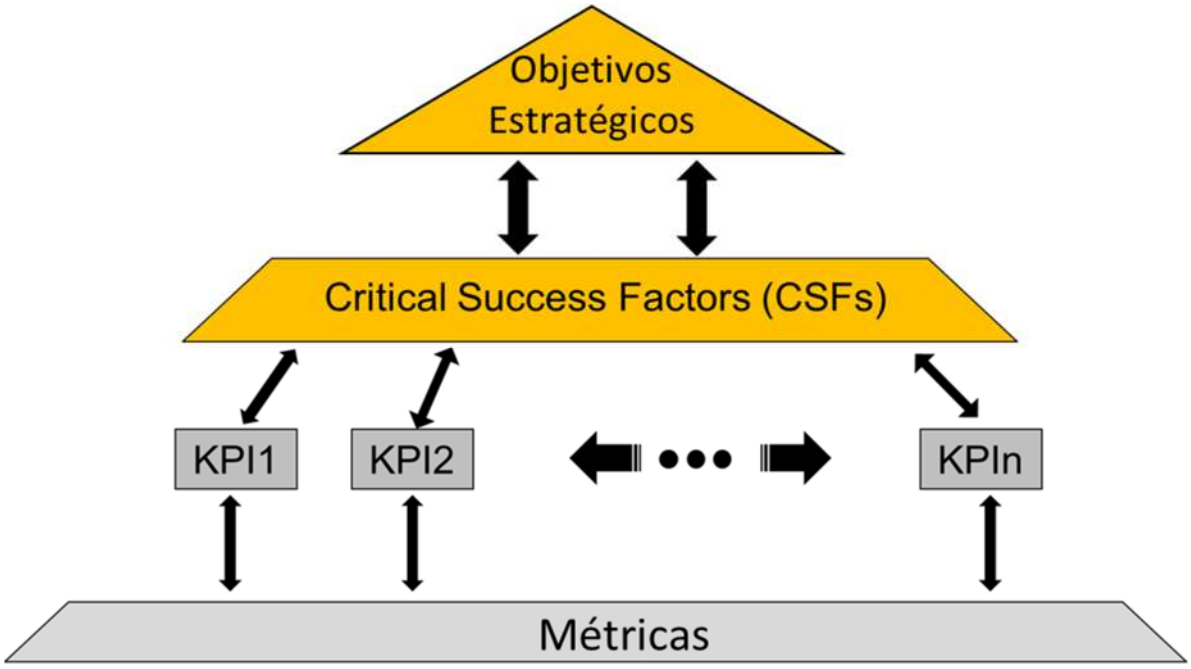

Tabla 3.58: Esquema de modelo de evaluación de los Objetivos Estratégicos. FUENTE PROPIA

Con la estructura presentada en la anterior figura, se pretende coordinar las actividades de la organización para la consecución de sus objetivos estratégicos, relacionándolos con los principales hitos del SGCN a los que deberían ir dirigidos los esfuerzos de la organización por tal de acometerlos: los “Factores Críticos de Éxito” (*CSFs*, del inglés *Critical Success factor*). Éstos CSFs, pueden estar vinculados a más de un objetivo estratégico y permiten establecer indicadores, o grupos de indicadores, que señalen el cumplimiento de las líneas estratégicas de la organización y el call center.

Los indicadores (*KPIs*, del inglés *Key Point Indicator*) son instrumentos que facilitan la toma de decisiones, ya que proporcionan una información relevante sobre la situación y evolución de la organización y permiten hacer un seguimiento de la eficacia del SGCN. Estos indicadores se obtienen a partir de las métricas, es decir,

a partir de la medida de las actividades llevadas a cabo en la operación habitual del ciclo de mejora del SGCN y que están vinculadas a la consecución de uno o varios CSFs.

Las características que deben tener los indicadores de cualquier SGCN son los siguientes:

- Ser medibles, la organización debe ser consciente de su grado de consecución a través de cuantificación y comparación en el tiempo con otros datos.
- Ser alcanzables
- Ser realistas, siendo fiables y proporcionando confianza
- Ser específicos

Las métricas son datos recogidos a través de la operación habitual de los procesos críticos del call center y que son fruto de la ejecución de las tareas del ciclo de mejora. Estas métricas alimentan los indicadores definidos con el fin de obtener el estado y evolución del SGCN, permitiendo analizar su evolución y el grado de adecuación con los objetivos estratégicos definidos.

El resultado de las métricas e indicadores debe medirse y reportarse periódicamente al promotor del SGCN, como mínimo en 3 ocasiones dentro de cada ciclo de mejora, para tener la capacidad de tomar decisiones si se detecta alguna evolución que previsiblemente incumpla algún hito significativo para el propio SGCN.

Debe determinarse la relación de cumplimiento de cada uno de los niveles de medida y evaluación (Objetivos Estratégicos, CSFs, indicadores y métricas), dependiendo del nivel de madurez del SGCN y de la exigencia de los requisitos de continuidad fijados en ejercicios anteriores de la implantación del mismo. Así pues, en un SGCN suficientemente maduro cabe pretender que el cumplimiento de los objetivos estratégicos se vea supeditado al cumplimiento del 100% de los CSF a los que se vean vinculados individualmente, y de manera homónima para CSF con indicadores e indicadores con métricas. En el caso de que la madurez del SGCN no permita realizar una relación tan exigente en el cumplimiento es posible determinar un cierto % a partir del cual cada objetivo estratégico tiene un resultado satisfactorio o definir algunos CSFs e indicadores como clave para el éxito de los objetivos estratégicos a los que estén vinculados.

3.15 Mejora

En esta sección se indica cómo tratar los diferentes acontecimientos que ocurran dentro de cada ciclo de mejora, incluyendo entre ellos los siguientes hitos:

- Revisión del SGCN
- Revisión específica de controles y procedimientos, ya sea de forma puntual o planificada, por parte del personal del call center con el objetivo de medir la eficacia y eficiencia del SGCN
- Detecciones puntuales de posibles mejoras por parte del personal del call center u otros departamentos y áreas ajenas al call center, dentro de la organización
- Auditorías internas o externas realizadas
- Resultados de métricas e indicadores

A partir de estos ejercicios se determinan las acciones y/o planes de acción que aseguren la mejora continua del SGCN. Dichas acciones pueden clasificarse entre correctivas o preventivas, según su origen. Debe determinarse en todo caso un responsable de cada acción o plan de acción a realizar, o más de uno, si se implica a diferentes áreas o departamentos internos o ajenos al call center. Seguidamente se describen las dos clasificaciones de acciones mencionadas:

a) Acciones Correctivas. Se trata de actuaciones que sirven para corregir incumplimientos detectados en controles de los estándares y/o legislación vigente aplicables a los servicios prestados por el call center incluidos dentro del alcance del SGCN. Las acciones correctivas se llevan a cabo para solucionar a lo que se designa como no conformidades mayores o menores, dentro de los procesos de auditoria del SGCN. En caso de tratarse de una no conformidad mayor, se considera que la causante de la misma es la ausencia o los fallos repetidos frente uno o más requerimientos de la norma ISO22301 o cuando se ponga en duda la capacidad del SGCN para alcanzar las directrices marcadas en la política de continuidad. Por otra parte, las no conformidades menores denotan un incumplimiento debido a una deficiencia menor o bien cuando uno o más elementos del SGCN se cumplen parcialmente

b) Acciones Preventivas. Son actividades que sirven para anticiparse a posibles futuros incumplimientos de la norma o para mejorar el SGCN dadas las oportunidades que se identifiquen en el análisis de contexto. Se trata de detectar aquellas desviaciones u omisiones en términos de continuidad que podrían suponer un comportamiento defectuoso del SGCN o de la continuidad de los procesos críticos de negocio del call center.

4. Conclusiones

Una vez concluida la implantación o mantenimiento de un SGCN, las principales conclusiones que se pueden extraer son:

- El call center tiene bajo control todos sus procesos críticos de negocio
- El call center está preparado para resistir y dar respuesta a los incidentes que ocurran, con afectación a la continuidad de negocio
- Los recursos de los que dispone el call center se destinan a los planes de acción determinados, de manera ordenada, priorizada y obteniendo un retorno de la inversión realizada aceptable.
- Ante la ocurrencia de un desastre, las implicaciones negativas de imagen, económicas y legales del call center se ven minimizadas
- El call center y sus órganos de gobierno toman las decisiones adecuadas y de manera eficiente cuando ocurre un desastre que afecta la continuidad de los procesos críticos
- El SGCN da valor añadido a los servicios prestados por el call center y aporta una mayor confianza de sus clientes y usuarios
- El call center está preparado para analizar e incluir nuevas amenazas y riesgos en el SGCN, a medida que el contexto de la organización cambia, adaptándose en todo momento

Todos los puntos mencionados se ven potenciados si se decide contar con los servicios de una entidad independiente y certificadora de este tipo de estándares (p.e. AENOR, BSI, etc), que aporta una visión objetiva y experta de las medidas llevadas a cabo, los ejercicios y actividades dentro del ciclo de mejora continua del SGCN.

5. Anexos

5.1 Amenazas y vulnerabilidades

El presente anexo contiene la relación entre las vulnerabilidades de los activos que participan en la operación de los procesos incluidos en el SGCN y las amenazas que las pueden explotar.

- Listado de amenazas: Se recoge en el siguiente documento adjunto un posible ejemplo de amenazas que pueden afectar a la continuidad de los activos necesarios para operar los procesos críticos del call center.

Listado de amenazas.xlsx

- Listado de vulnerabilidades: Se recoge en el siguiente documento adjunto un posible ejemplo de vulnerabilidades que pueden ser explotadas en los activos necesarios para operar los procesos críticos del call center.

Listado de vulnerabilidades.xlsx

5.2 Estrategias de recuperación del CPD

Las estrategias de recuperación en caso de desastre se pueden catalogar según el grado de disponibilidad de los equipos en un CPD alternativo, lo cual determina la rapidez de respuesta frente la interrupción de un servicio.

Tipo	Descripción	Disponibilidad de los sistemas	Coste	Requerimientos de mantenimiento y administración
Mirror Site	Sala con equipos técnicos operativos y datos actualizados	Minutos 0 – 5	Muy Alto	Muy Alto
Hot Site	Sala con equipos técnicos operativos	Minutos 5 – 240	Alto	Alto
Warm Site	Sala con equipos técnicos	Horas 1 – 24	Medio	Medio
Cold Site	Sala vacía acondicionada	Días	Bajo	Bajo

Tipo	Descripción	Disponibilidad de los sistemas	Coste	Requerimientos de mantenimiento y administración
		1 – 7		

- Cold Site: Es una sala vacía preparada con condiciones ambientales y de seguridad para acoger equipos informáticos y de comunicaciones. Esta estrategia es válida para procesos de negocio con un RTO poco exigente que permitan un margen de tiempo suficiente para adquirir y poner a punto los equipos. Los costes son bajos ya que sólo se incurre en gastos en caso de ocurrencia de un desastre. No requiere esfuerzo de mantenimiento ni de administración, solo es necesario definir el plan el tipo de hardware que sería necesario en caso de desastre.
- Warm Site: Sala preparada con condiciones ambientales y de seguridad con equipos informáticos y de comunicaciones instalados pero no operativos. Permite utilizar equipos reemplazados por obsolescencia si la capacidad necesaria puede ser menor que la que se presta en condiciones de normalidad.
- Hot Site: Sala preparada con condiciones ambientales y de seguridad con equipos informáticos y de comunicaciones instalados y operativos pero sin datos o datos no actualizados. Esta estrategia se recomienda en caso de un RTO relativamente exigente (5-240 minutos). En caso de desastre, solo es necesario actualizar los datos y redirigir los servicios a esta ubicación de respaldo. Requiere costes de mantenimiento y administración más altos por necesitarse la actualización de la plataforma de manera continua para que se cumplan las mismas condiciones que en el CPD original.
- Mirror Site: Sala preparada con condiciones ambientales y de seguridad con equipos informáticos y de comunicaciones completamente operativos y datos actualizados. Esta estrategia se recomienda en caso de un RTO muy exigente (0 - 5 minutos) donde la tolerancia de interrupción de los servicios es mínima. Esta opción implica unos costes muy altos en tecnología, administración y mantenimiento además de un incremento en la complejidad de la operatividad, pues implica el uso de sistemas de activación automáticos o balanceo de cargas de trabajo.

5.3 Estrategias de recuperación de datos

Las estrategias de recuperación en caso de desastre se pueden catalogar según el grado de disponibilidad de datos en un CPD alternativo, lo cual determina la calidad de datos que se pueden recuperar.

Tipo	Descripción	RPO	Coste	Requerimientos de mantenimiento i administración
Mirroring	Replicación síncrona	Horas 0 – 3	Muy Alto	Muy Alto
Shadowing	Replicación asíncrona	Horas 1 – 24	Alto	Alto
Remote copy	Copia electrónica de datos	Horas 8 – 24	Medio	Medio
Conventional Backup	Externalización de los soportes de backup (diariamente)	Días 1 – 3	Medio	Bajo

- Replicación: Es el proceso de escribir los datos en el servidor principal y al de respaldo de forma simultánea. Usualmente se utiliza tecnología SAN (Storage Area Network): cabinas de discos conectadas por fibra Óptica (conexión dedicada).
  - **Mirroring (síncrono)**: El dato no se llega a escribir hasta que se tenga la aceptación de ambos servidores. Este método es recomendable en caso de requerir un RPO casi cero que implica un "zero data loss". Los inconvenientes que aporta son: degradación del rendimiento, no es recomendable con grandes volúmenes de datos, largas distancias, anchos de banda pequeños o con mucha latencia.
  - **Shadowing (asíncrono)**: Los cambios se recogen en forma de logs que periódicamente se aplican al servidor de respaldo. El RPO está formado por lo ultima transmisión y la aplicación de los cambios, por lo tanto, es peor que en el caso del Mirroring, pero no tiene ninguno de sus inconvenientes.
- Remote Copy: Transmisión de los datos por la red WAN de forma automática al servidor de respaldo, teniendo así el backup offsite (esto ahorra el transporte de los soportes). Este método proporciona un buen RPO al tener los datos de forma rápida al servidor de respaldo, además permite incrementar la frecuencia de las copias (2 o 4 veces diarias)

dependiendo del volumen de datos a proteger y si se utiliza el método incremental.

- Conventional Backup: Es el método de realizar copias de seguridad de varios servidores en soportes y enviarlos al lugar de respaldo, o contratar un proveedor externo que los almacene adecuadamente. En este caso el RPO depende de la frecuencia en la que se externalizan los soportes (diaria – semanal).

6. Referencias

- Norma ISO22301


Norma ISO 22301.pdf

- Suplemento de London Times sobre Resiliencia


Forward thinking organisation seeks re:

- Informe Gartner sobre estrategias de continuidad


Gartner - Strategies for Achieving Continuc

- Informe Horizon Scan 2016


Informe Horizon Scan 2016.pdf

- Publicación sobre resiliencia de Cranfield School of Management


roads-to-resilience.pdf

- Fuente de la figura 2.1: http://clasificaciondelostiposdeorganizacion.blogspot.com.es/2015/06/que-es-una-es-un-grupo-social.html

- Fuente de la figura 2.6: http://www.grandespymes.com.ar/2013/02/16/cuadro-de-mando-integral-en-tu-negocio/

- Fuente de la figura 3.4: http://www.uniatlantico.edu.co/uatlantico/noticias/convocatoria-p-blica-n-001-2013-2-personal-de-apoyo-vicerrector-de-docencia

- Fuente de la figura 3.56: http://www.idi.edu.pe/#!GESTI%C3%93N-DEL-CONOCIMIENTO/c144z/410FCB66-A506-44D8-8CA2-F5AA05A2BBFD